

User Guide

hp StorageWorks Fabric Manager Version 4.2.x

Fourth Edition (September 2004)

Part Number: AA-RUQSD-TE

This document provides procedures for SAN administrators to set up and manage HP StorageWorks SANs. Fabric Manager allows you to manage the switches in your SANs from a single user interface. With this software, you can configure any aspect of the switches in your SAN.



© Copyright 2004 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft®, Windows®, Windows NT®, and Windows XP® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Linux® is a U. S. registered trademark of Linus Torvalds.

Java™ is a US trademark of Sun Microsystems, Inc.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for Hewlett-Packard Company products are set forth in the express limited warranty statements for such products. Nothing herein should be construed as constituting an additional warranty.

Printed in the U.S.A.

Fabric Manager Version 4.2.x User Guide
Fourth Edition (September 2004)
Part Number: AA-RUQSD-TE



contents

About this Guide.	15
Audience.	15
Related Documentation	15
Conventions	15
Document Conventions	16
Text Symbols	16
Getting Help	17
HP Technical Support	17
HP Storage Web Site	17
HP Authorized Reseller	17
1 About Fabric Manager	19
Introduction.	19
New Features in this Release	19
Changed Features in this Release	20
Using Fabric Manager	21
Fabric Manager Graphical User Interface	21
Address Field	22
Standard Fabric Manager Icons and Windows	22
At-A-Glance Windows in the Overview View	24
View Selector Bar	24
ID Menu	25
SAN Elements Tab.	25
Filter Tab	26
Storing Data	26
Persistent Files	26
System Requirements	27
Client and Server Machines	27
Windows Environments	27
Solaris Environments.	28
Supported Devices	28
Supported Operating Systems.	28
Fabric Manager Client	28
Fabric Manager Server.	29
Firmware Specific Features	29

2	Installing and Upgrading	31
	Installing Fabric Manager	32
	Full Version	32
	Evaluation Version	32
	Installing the Client and Server Together or Installing Server Only	33
	Installing Fabric Manager Client Only	36
	Upgrading Fabric Manager	37
	Launching Fabric Manager for the First Time	39
	Registering Fabric Manager	40
	Uninstalling Fabric Manager	40
	Windows Operating Systems	40
	Solaris Operating Systems	40
3	Fabric Management	41
	Discovering a Fabric	41
	Running a Subnet Scan (Fabric Scan)	41
	Deleting a Fabric	42
	Renaming a Fabric	42
	Renaming a Switch	43
	Renaming a Port	43
	Renaming a Device Node and Device Port	43
	Customizing a View	45
	Disabling Table View Tooltips	47
	Copying Fabric Manager View Information to Spreadsheet Applications	47
	Printing Fabric Manager View Information	47
	Saving Fabric Manager View Information	47
	Changing At-A-Glance Window Descriptions	48
	Logging In to Multiple Devices Simultaneously	48
	Disabling Passwords from Being Saved to the Server	49
	Displaying SAN Elements by IP address, Domain ID, WWN, and Name	50
	Enabling and Disabling Elements	50
	Setting the Log Level	50
	Downloading a Configuration	51
	Downloading to Switches from a Baseline File	51
	Downloading to Switches from a Baseline Switch	52
	Configuring File Transfer Options	52
	Configuring Notification Parameters	53
	Synchronizing Time and Date Across a Fabric	53
	Filtering Elements	54
	Designating a Switch as a Core Switch	54
	Monitoring Link Performance	55
	Setting the Link Threshold Percent	55
	Setting the Link Trigger Period	55
	Opening a Telnet Session for a Nonsecure Switch	55
	Displaying the Switch Health Report	56
4	Fabric Events	57
	Viewing Fabric Events with Events View	57
	Refreshing Fabric Events	57
	Filtering Fabric Events	57

5	Using the Fabric Watch Module in Fabric Manager.	59
	Fabric Watch Terms	60
	How Fabric Watch Works	60
	Using Fabric Watch	60
	Launching the Fabric Watch Module	61
	Viewing Alarms	61
	Configuring Threshold Boundaries and Alarms.	61
	Configuring the Email Server on a Switch.	62
	Configuring the Email Alert Recipient.	62
	Enabling and Disabling Threshold Alarms.	63
	Configuring Threshold Behavior	63
	Displaying a Fabric Watch Alarm Configuration Report.	64
	Fabric Watch Dialog Box Reference	64
	Alarm Notification Tab.	64
	Threshold Configuration Tab	65
	Area Configuration Tab	66
	Element Configuration Tab	66
	Configuration Report Tab	67
	Email Configuration Tab	67
6	Change Management	69
	Change Management Profiles	70
	Snapshot Reports	70
	Configuring Notification Parameters	71
	Creating a CM Profile.	71
	Displaying Saved CM Profiles	73
	Deleting CM Profiles	73
	Editing CM Profiles	74
	Duplicating (Cloning) Existing CM Profiles	74
	Displaying a Change Report.	75
	Creating CM Snapshots on Demand.	76
	Comparing Two CM Snapshots to Each Other	76
	Exporting CM Snapshot Reports and Change Reports.	76
	Displaying CM Change Reports (XML Format) in External Applications	76
	Printing CM Snapshot and Change Reports	77
	Changing Baseline Snapshot Reports.	77
7	Name Server	79
	Displaying Name Server Entries	81
	Displaying Name Server Information for a Device	81
	Displaying Zone Members of a Device	81
8	Fabric Topology	83
	Links	84
	Viewing Your Fabric with Topology View	85
	Assigning a Core Switch Manually	85
	Configuring Topology View Options.	86
	Viewing Discovered Fabric Topologies	86
	Taking a Snapshot of a Topology.	87
	Moving a Topology Object.	87

9	Comparing Configurations	89
	Best Practices	90
	Saving a Baseline Configuration to a File	90
	Comparing Switches to a Baseline	91
	Comparing Switches to a Baseline File	91
	Comparing Switches to a Baseline Switch	92
	Customizing Baseline Templates	93
	Anatomy of Template Files	94
	Description Tag	94
	The section Tag	95
	The prefix Tag	96
	Creating or Editing a Template	97
10	Fabric Merge Check	99
	Comparing Fabrics for a Fabric Merge	100
11	Licensing	101
	Introduction	101
	Exporting and Importing License Keys	102
	Exporting License Keys from Switches to a File	102
	Importing License Keys from a File to a Switch	102
	Removing a License Key from a Switch	102
	Performing E-Licensing	103
	Obtaining Licenses from Transaction Keys	103
12	Downloading Firmware	105
	Performing a Firmware Download to Multiple Switches	106
	Controlling Firmware Download Reboots	107
13	Sequenced Reboots	109
	Creating a Reboot Group	110
	Assigning Switches to a Reboot Group	111
	Creating Single Switch Reboot Groups	111
	Performing a Sequenced Reboot	112
14	Working with Switch and Port Groups	113
	Creating Switch Groups	114
	Creating Port Groups	114
	Editing a Switch or Port Group	115
	Deleting a Switch or Port Group	115
15	Managing Alerts	117
	Switch Status Change Alerts	117
	Switch Unreachable Alerts	117
	Change Management Triggered Alerts	118
	Identifying Switches and Fabrics with Alerts	118
	Acknowledging Alerts	119
	Resolving Alerts	119
	Deleting Alerts	119

16 Call Home	121
Configuring Call Home	122
Editing Configurations	124
Globally Enabling or Disabling Call Home	124
17 Performance Monitoring	125
Granularity	125
Reports	126
Graphs	127
Templates	127
Enabling Performance Monitoring	128
Disabling Performance Monitoring	128
Generating Custom Performance Monitor Reports	129
Performance Monitor Reports	129
Generating Custom Performance Monitor Graphs	132
Generating Performance Monitor Reports from Saved Templates	134
Creating Performance Monitor Report Templates	135
Saving Performance Monitor Reports and Graphs	135
Printing Performance Monitor Reports	136
Exporting Performance Monitor Reports	136
Displaying Saved Performance Monitor Reports and Graphs	136
Deleting Performance Monitor Reports and Graphs	136
Generating Custom Performance Monitor Graphs	137
Generating Performance Monitor Graphs from Templates	138
Editing Performance Monitor Graphs	138
Displaying Performance Monitor XML Reports in External Applications	139
18 Using Fabric Manager With the MP Router	141
Sharing Devices Between Fabrics	142
Connecting Edge Fabrics	143
Displaying Logical SANs	144
19 FDMI-Capable HBA Firmware Download	145
Downloading Firmware to an HBA	145
20 Security	147
Security Levels	148
Creating a Secure Fabric	150
Launching the Policy Editor	152
Viewing and Configuring Security Policy Options	152
Configuring FCS Policy Options	152
Configuring SCC Policy Options	154
Configuring Telnet, RSNMP, WSNMP, HTTP, and API Policy Options	155
Configuring RSNMP Policy Options	157
Configuring WSNMP Policy Options	157
Configuring HTTP Policy Options	158
Configuring API Policy Options	159
Configuring DCC Policy Options	160
Configuring MS Policy Options	161
Configuring Serial and Front Panel Policy Options	162

Configuring Front Panel Policy Options	163
Configuring No Node WWN Zoning	164
Changing the FCS or Non-FCS Admin Security Password	164
Telnet on a Secure Fabric	165
Opening a Telnet Session for a Secure Fabric	165
Merging Secure Fabrics	166
Adding a Switch to a Secure Fabric	166
21 Using the Zoning Module in Fabric Manager	167
Zone	167
Alias	168
Configuration	168
Zoning Schemes	168
Security	168
Zoning Methods	168
Zoning Method and Tabs Available	169
Accessing the Zone Administration Module	169
Creating a Zone Configuration	169
Sample Configuration	170
Displaying the Enabled Zone Configuration	171
Displaying the Zone Configuration Summary	171
Adding a WWN to the Zoning Database	171
Deleting a WWN from the Zoning Database	171
Replacing a WWN in the Zoning Database	172
Searching for a Zone Member	172
Selecting a Zoning Method	172
Refreshing the Fabric	173
Enabling a Zone Configuration	173
Disabling a Zoning Configuration	174
Saving Changes to an Existing Configuration	174
Refreshing the Zoning Database	174
Clearing the Zoning Database	175
Creating a Zone Alias	175
Modifying the Members of a Zone Alias	176
Deleting a Zone Alias	176
Renaming a Zone Alias	176
Creating a Zone	177
Modifying the Members of a Zone	177
Deleting a Zone	178
Renaming a Zone	178
Creating a QuickLoop	178
Modifying QuickLoop Members	179
Deleting a QuickLoop	179
Renaming a QuickLoop	180
Creating a Fabric Assist Zone	180
Adding and Removing Fabric Assist Zone Members	180
Deleting a Fabric Assist Zone	181
Renaming a Fabric Assist Zone	181
Adding and Removing Zone Configuration Members	181
Deleting a Zone Configuration	182

Renaming a Zone Configuration	182
Creating a Configuration Analysis Report	182
Zoning Reference	183
File Menu	183
Edit Menu	184
View Menu	184
Actions Menu	185
Alias Tab	185
Alias Tab Descriptions	186
Zone Tab	187
Zone Tab Descriptions	188
QuickLoop Tab	189
QuickLoop Tab Descriptions	190
Fabric Assist Tab	190
Fabric Assist Tab Descriptions	191
Config Tab	192
Config Tab Descriptions	193
22 Troubleshooting	195
Checking Fabric Manager	196
Checking the Client Side	196
Authentication Issues (Unable to Log in)	196
Client Access to Switches	197
Client-Side CPU Usage	197
Capturing and Reporting Client-Side Issues	197
Checking Client/Server Interaction	198
No Client/Server Interaction	198
Client/Server Version Mismatch	198
Determine Client or Server Problem	198
Checking the Server Side	199
Server Cannot Access Switches	199
Server-Side CPU Usage	199
Capturing and Reporting Server-Side Issues	199
Checking Fabric Discovery Problems	199
Saving the SupportShow Command Output	201
Pinpointing Additional Problem Areas	202
Installing Fabric Manager Client on Solaris Using BASH as Default Shell	202
Cannot Locate Fabric Manager License Key and Serial Number	202
Switches and Hosts No Longer Recognize an HBA After Firmware Download to HBA	202
503 Service Unavailable/Overloaded Error	202
Installation Wizard Does Not Launch	202
Installation Wizard Locks Up	202
Incorrect Performance Monitoring Port Statistics	203
A File Menu Reference	205
Introduction	205
Fabric Login Window	206
Groups Submenu	207
Edit Switch Groups Window	207
Edit Port Groups Window	208

Options Window	208
Topology Options	209
File Transfer Options	210
B Edit Menu Reference	211
Edit View Options Windows	212
C View Menu Reference	213
Introduction	214
Table-Format View Buttons	214
Overview View	215
Fabric At-A-Glance Windows	216
Switch At-A-Glance Windows	216
Port At-A-Glance Windows	217
SwitchGroups At-A-Glance Windows	217
PortGroups At-A-Glance Windows	217
Alerts View	217
Topology View	218
Switches View	219
Ports View	220
Device Ports View	221
Devices View	223
Portgrid View	223
LSAN View	223
LSAN Info View	224
Physical Devices Tab	224
Virtual Devices Tab	224
LSAN Information Tab	225
D Actions Menu Reference	227
Introduction	227
Fabric Actions	227
Security Admin Window	228
Switch Actions	230
Port Actions	230
E Topology Menu Reference	231
F Tools Menu Reference	233
Introduction	233
Reboot Submenu	234
Config Submenu	234
Licensing Submenu	235
Change Management Submenu	235

G Help Menu Reference 237

Index 239

Figures

1	Fabric Manager GUI Overview	22
2	Fabric At-A-Glance Window.....	24
3	View Selector Bar	24
4	Fabric Manager Evaluation Installation Version Warning	32
5	Fabric Manager Evaluation Installation Version Expiration Error	33
6	Device Ports Screen	44
7	Renaming a Device Port.....	44
8	Importing Alias Names	45
9	Options Dialog Box	49
10	Time Dialog Box	54
11	Change Management Snapshot Items	72
12	Change Management Change Report.....	75
13	Template Selection.....	93
14	Parameter Selection	94
15	Description Change Results.....	95
16	Section Change Results	96
17	Prefix Change Results	97
18	Firmware Download to Switches Window	106
19	Call Home Window	122
20	Call Home Configuration.....	123
21	Using Performance Monitor Graphs	127
22	Configuring Custom Performance Monitor Reports	129
23	Selecting Ports for Custom Performance Monitor Reports	130
24	Performance Monitor Report Displayed in HTML Format.....	131
25	Configuring Custom Performance Monitor Graphs.....	132
26	Performance Monitor Graph	134
27	Sample Meta SAN Including MP Routers.....	141
28	Selecting Devices to Share Dialog.....	142
29	Select FC Router	143
30	Policy Editor.....	147
31	Select FCS Switches	150
32	Select Security Policy Settings (Optional).....	151
33	Configuring the FCS Policy.....	153
34	Configuring the SCC Policy.....	154
35	Configuring the Telnet Policy	155
36	Configuring the DCC Policy	160
37	Configuring the Serial Policy.....	162
38	Configuring the FCS or Non-FCS Admin Security Password.....	165
39	Alias Tab in the Zone Administration Window.....	185
40	Zone Tab in the Zone Administration Window.....	187
41	QuickLoop Tab in the Zone Administration Window.....	189
42	Fabric Assist Tab in the Zone Administration Window	191
43	Config Tab in the Zone Administration Window	192
44	Fabric Manager Server (Services Window).....	201
45	Database (Services Window).....	202

Tables

1	Document Conventions	16
2	Standard Icons	23
3	Fabric Manager Views	25
4	Fabric Manager 4.2.x Persistent Files	27
5	Firmware-Specific Features	29
6	Upgrading Fabric Manager From a Previous Version	38
7	Event Log Table Fields	58
8	Fabric Watch Terms and Definitions	60
9	Fabric Watch Dialog Box Components	64
10	Alarm Notification Tab Component Descriptions	65
11	Threshold Configuration Tab Components	65
12	Area Configuration Components	66
13	Element Configuration Tab Components	66
14	Threshold Configuration Report Component Descriptions	67
15	Email Configuration Component Descriptions	67
16	Name Server Table Entries	80
17	Topology View Link Images	84
18	Baseline Sources	89
19	Sequenced Reboot Options	109
20	Stored Samples for Granularity Options	126
21	Default Performance Monitoring Report Templates	128
22	High Security-Level Settings Per Policy	148
23	Medium Security-Level Settings Per Policy	149
24	Low Security-Level Settings Per Policy	149
25	Zoning Methods	169
26	Zone Methods and Tabs Table	169
27	Sample Zoning Database	170
28	Zone Administration Window Components	183
29	File Menu Options	183
30	Edit Menu Options	184
31	View Menu Options	184
32	Actions Menu Options	185
33	Alias Tab Component Descriptions	186
34	Zone Tab Component Descriptions	188
35	QuickLoop Tab Component Descriptions	190
36	Fabric Assist Component Descriptions	191
37	Config Tab Component Descriptions	193
38	File Menu Options	205
39	Fabric Login Window Components	206
40	Groups Submenu Items	207
41	Edit Switch Groups Window Components	207
42	Edit Port Groups Window Components	208
43	Options Categories	208
44	Topology Options	209
45	File Transfer Options	210
46	Edit Menu Options	211
47	Selection of Views Available at Various Levels of SAN Hierarchy	214
48	Table-Format View Buttons	215
49	SAN Node Icons	215

50	Fabrics Node Icons	216
51	Switch At-A-Glance Icons	216
52	Port At-A-Glance Switch Detail Icon	217
53	SwitchGroups Detail Icons	217
54	PortGroups Detail Icons	217
55	Alerts View Display	218
56	Topology View Icons	218
57	Switches View Display	219
58	Ports View Display	221
59	Device Ports View Display	221
60	Devices View Display	223
61	LSAN View Display	223
62	LSAN View Physical Devices Tab	224
63	LSAN View Virtual Devices Tab	224
64	LSAN View LSAN Information Tab	225
65	Fabric Actions	228
66	Security Admin Window Objects	228
67	Switch Actions	230
68	Port Actions	230
69	Topology Menu Options	231
70	Tools Menu Options	233
71	Reboot Submenu Options	234
72	Config Submenu Options	234
73	Licensing Submenu Options	235
74	Change Management Submenu	235
75	Help Menu Options	237

About this Guide

This user guide provides comprehensive information to help you administer, operate, maintain, and troubleshoot HP StorageWorks Fabric Manager 4.2.x (note that 4.2.x designates versions 4.2.0 and later).

The major topics discussed in this chapter are:

- “[Audience](#)” on page 15
- “[Related Documentation](#)” on page 15
- “[Conventions](#)” on page 15
- “[Getting Help](#)” on page 17

Audience

This document is intended for use by systems administrators and technicians.

Related Documentation

For the latest information, documentation, and firmware releases, visit the HP StorageWorks web site: <http://www.hp.com/country/us/eng/prodserv/storage.html>.

To access the technical documentation:

- Locate the **networked storage** section of the web page.
- Under **networked storage**, go to the **by type** subsection.
- Click **SAN infrastructure**. The SAN infrastructure page is displayed.
- Locate the **fibre channel switches** section.
- Click the appropriate product name. The product overview page is displayed. Go to the **product information** section.
- Click **technical documents**.

For information about Fibre Channel standards, visit the Fibre Channel Industry Association web site, located at <http://www.fibrechannel.org>.

Conventions

Conventions consist of [Document Conventions](#) and [Text Symbols](#).

Document Conventions

The document conventions specified in [Table 1](#) apply in most cases.

Table 1: Document Conventions

Element	Convention
Cross-reference links	Blue text: Figure 1
Menu items and buttons; key, tab, and box names (not window and dialog box titles)	Bold
Text emphasis and document titles (not CD titles) in body text	<i>Italics</i>
User input, commands, code, file, and directory names; and system responses (output and messages)	Monospace font
Command-line and code variables	<i>Monospace, italic font</i>
Web site addresses	Blue, underlined font: http://www.hp.com

Text Symbols

The following symbols may be found in the text of this guide. They have the following meanings.



WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.



Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Getting Help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: <http://www.hp.com>.

HP Technical Support

Telephone numbers for worldwide technical support are listed on the following HP web site: <http://www.hp.com/support/>. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP Storage Web Site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: <http://www.hp.com/country/us/eng/prodserv/storage.html>. From this web site, select the appropriate product or solution.

HP Authorized Reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, refer to the HP web site for locations and telephone numbers: <http://www.hp.com>.

About Fabric Manager

1

Introduction

Fabric Manager allows you to manage the switches in your storage area networks (SANs) from a single user interface. With this software, you can configure any aspect of your SAN.

Use Fabric Manager to configure multiple switches and the MP Router simultaneously from one location, view the status of multiple devices in one window, and perform SAN-level maintenance without accessing switch after switch.

Fabric Manager provides high-level information about all switches in the fabric, launching the Advanced Web Tools application when more detailed information is required. The Advanced Web Tools launch is transparent, providing a seamless user interface. All devices in the fabric are represented in the main window of Fabric Manager and can be managed through Fabric Manager, including the MP Router.

Fabric OS supports a maximum of five simultaneous HTTP sessions to any one switch. HTTP sessions are leveraged by every copy of Fabric Manager server and Advanced Web Tools that is monitoring any one switch.

The Fabric Manager graphical user interface (GUI) uses icons and menus to help you more quickly and easily administer your SANs. This chapter identifies the visual elements that you see when you launch Fabric Manager.

New Features in this Release

The following features are new in this release of Fabric Manager:

- The Change Management feature is a new feature that allows you to monitor specific changes in the fabric by taking snapshots at scheduled intervals and comparing the snapshots to a baseline snapshot. You can export XML versions of the change reports (comparison between baseline snapshot and subsequent snapshot). You can also configure the Change Management feature to trigger alerts in the Alerts view and send email notifications to a specified user email address. For more information, see [Chapter 6, “Change Management.”](#) The Change Management feature replaces the features for Fabric Checking, ISL Checking, and Fabric Backup/Diff from previous versions of Fabric Manager.
- Fabric Manager provides MP Router support by allowing you to share devices between two or more fabrics, configure EX_Ports on one or more MP routers, display logical SANs in the Topology view, and display logical SAN information in the new LSAN view. For more information, see [Chapter 18, “Using Fabric Manager With the MP Router.”](#)

- Fabric Manager allows you to save `supportShow` command output for one or more switches in a fabric as text files. These files can be used for troubleshooting. For more information, see [“Saving the SupportShow Command Output”](#) on page 201.
- The Performance Monitoring feature is a new feature that allows you to capture port traffic and store it to the Fabric Manager database. You can generate reports and graphs based on the stored data. For more information, see [Chapter 17, “Performance Monitoring.”](#)
- Fabric Manager has a new view, Alerts view, that displays switch status change alerts, switch unreachable alerts, and Change Management triggered alerts. You can easily identify switches and fabrics with alerts in the **SAN Elements** tab and the At-A-Glance windows, as they are identified with an **Alert** icon.
- Secure Fabric OS Management allows you to create a secure fabric. You can define the Fabric Configuration Servers (FCS) switch list, set new passwords, and define new policies for various accounts for FCS and non-FCS switches. See [Chapter 20, “Security”](#) for more information.
- Device node and device port name support allows you to import names for devices from the zone aliases defined in the zoning database on a fabric. You can also rename the devices manually. The devices are identified by their new name attribute wherever they are displayed in Fabric Manager screens (for example, the share device wizard, LSNs display, device ports table, device node table). See [Chapter 3, “Fabric Management”](#) for more information.

Changed Features in this Release

The following features are changed in this release of Fabric Manager:

- In previous versions of Fabric Manager, fabric lists, switch groups, and port groups were user-level, and only one user could see them. From this release onward, fabrics and switch port groups are global to all users on the server, and the information is stored on the server database, so all users share fabric and switch and port group information. In addition, all discovered fabrics are saved to the Fabric Manager server and are available to all clients using that server.
- In previous versions of Fabric Manager, you were asked for a server email address during the installation. Now, you can configure notification parameters after the Fabric Manager installation using the Notification Configuration feature in the **Tools** menu. For more information, see [“Configuring Notification Parameters”](#) on page 53.
- General usability enhancements include the following:
 - Security Feature: In addition to the new security features, the security policy editor has been improved for usability.
 - General Table Enhancements: All views (except Overview view and Topology view) have view options and sort order buttons in the view, making it easier to customize the information displayed in the view. You can now do multi-column sorting, and all table views have tooltip information available.
 - Summary and Detail views are replaced with the Overview view.
 - Call Home GUI has been enhanced by providing a wizard to manage call home configurations.
- Alerts view information replace status reason in the Events view.

- General scalability enhancements include the following:
 - Client-Server Architecture: The Client-Server architecture is enhanced to move the data collection and aggregation functionality to the server (supporting the global fabric and switch/port group information), and event based updates are at the client level.
 - Polling algorithms are improved.
 - The selection of views displayed at various levels of SAN hierarchy is improved for usability.
- The Overview view replaces the previous Fabric Manager Detail and Summary views.

Using Fabric Manager

When you click an element in the SAN Elements tab, Fabric Manager displays information about all immediately-subordinate elements in the hierarchy. For instance, if you click **My SAN** from the SAN Elements tab, Fabric Manager displays summaries for Fabrics, Switch Groups, and Port Groups. If you click a particular fabric in the hierarchy, Fabric Manager displays information on each switch in the fabric. If you click a particular group, Fabric Manager displays information on each member of the group.

Each Fabric Manager view displays different information. You can customize which information is displayed, and the order in which the information is displayed. For more information on selecting views, see “[View Selector Bar](#)” on page 24. For information on customizing views, see “[Device Ports Screen](#)” on page 44.

As you move from view to view and element to element, Fabric Manager tracks your views so you can use the navigation icons to move back and forth between the selections that you made from the **View** menu or view selector. Use the navigation icons to move forward and backward through views that you have already accessed. See [Table 2](#) on page 23 for a description of the navigation icons.

Fabric Manager Graphical User Interface

The Fabric Manager GUI includes standard menus, tabs, icons, and windows. [Figure 1](#) shows the basic Fabric Manager interface.

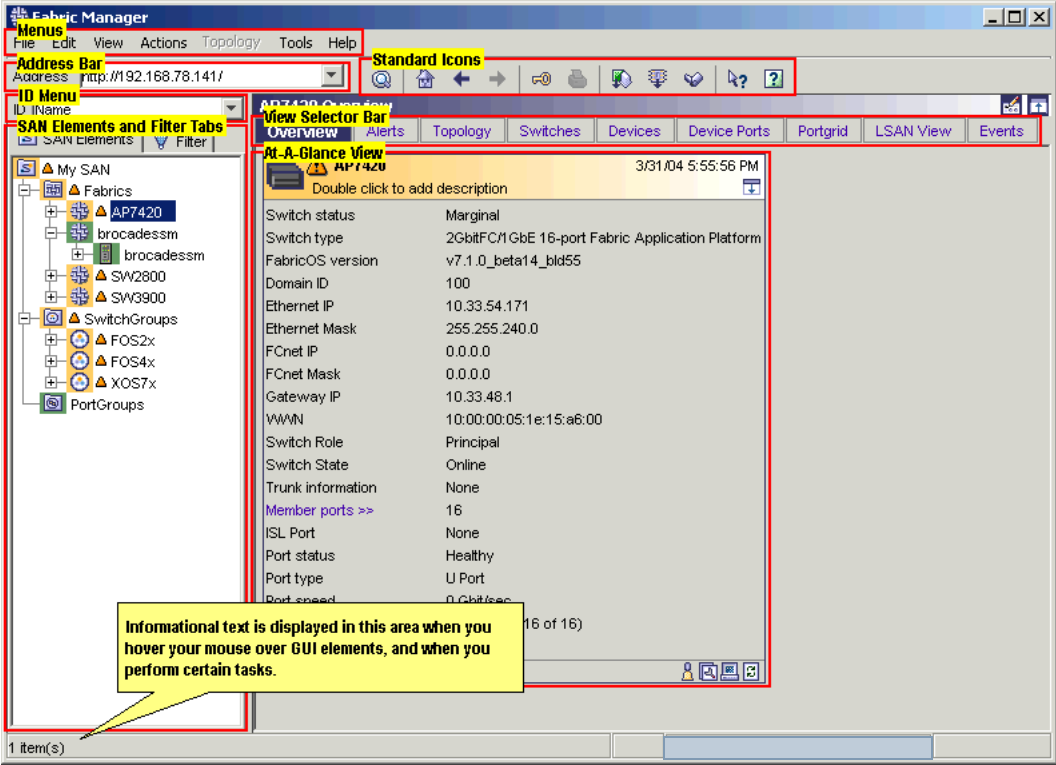


Figure 1: Fabric Manager GUI Overview

The following sections provide an overview of the menus, tabs, icons, and windows.












Address Field

Use the Address Field to discover a new fabric. The Address Field has a menu of the fabrics that you have discovered and lets you enter the IP address or switch name of new switches and fabrics that you want to monitor.

Standard Fabric Manager Icons and Windows

Standard icons appear in the Fabric Manager display; different windows display when you use the Overview view, depending on which element you select from the **SAN Elements** tab. [Table 2](#) describes the standard Fabric Manager icons. Additional icons display in the Topology view; you can find descriptions of those icons in [Appendix C](#).

Table 2: Standard Icons

Name	Icon	Description
Subnet scan		Opens the Subnet scan dialog box to help you discover fabrics. For more information, see “Running a Subnet Scan (Fabric Scan)” on page 41.
Home		Navigation icon: Returns to the view that appeared when you opened Fabric Manager.
Previous		Navigation icon: Returns to the previous view in the navigation history (if applicable). If you click the Previous icon for more than half a second, a menu showing the previous 10 views are displayed. You can select one of the views or select cancel.
Next		Navigation icon: Moves forward to the next view in the navigation history (if applicable). If you click the Next icon for more than half a second, a menu showing the previous 10 views are displayed. You can select one of the views or select cancel.
Fabric login		Opens the Fabric login dialog box so you can log in to one or more switches. For more information, see “Logging In to Multiple Devices Simultaneously” on page 48.
Print		Prints the contents of the view. The Print icon is available from all views except the Overview view. For all table-format views, clicking the Print icon prints the information in the table. For the Topology view, the Print icon prints the graphical information currently displayed in the Topology view.
Firmware download to HBAs		Opens the Firmware download to HBAs dialog box. For more information, see “Downloading Firmware to an HBA” on page 145.
Firmware download to switches		Opens the Firmware download to switches dialog box. For more information, see Chapter 12 .
Sequenced reboot		Opens the Sequenced reboot dialog box. For more information, see Chapter 13 .
Context Help		Changes your pointer to the help pointer. Click an element of the GUI for context-sensitive help.
Help		Opens Fabric Manager Online Help.

At-A-Glance Windows in the Overview View

The “[Overview View](#)” on page 215 describes information about elements in the [SAN Elements Tab](#). Each element has an At-A-Glance window in the Overview view. [Figure 2](#) displays an example of an At-A-Glance window for a fabric called Web185 in the Overview view.



Figure 2: Fabric At-A-Glance Window

At-A-Glance windows display information about the element and icons that you can use to monitor and configure that element. The background color of the At-A-Glance view for each element indicates the physical status of that element, where:


- Green indicates the element is healthy
- Yellow indicates the element is marginal
- Red indicates the element is critical
- Gray indicates the element is unknown or unmonitored

View Selector Bar

The “[View Selector Bar](#)” on page 24 provides access to all of the views available for the element you have selected. Different views are available, depending on the element you have selected from the “[SAN Elements Tab](#)” on page 25. There are two ways to access different views from Fabric Manager:

- Select **View > View Type**, where *View Type* is the view that you want to access.
- Use the “[View Selector Bar](#)” on page 24.

To use the View Selector bar:

1. Click the **Display View Selector** icon () in the top right corner of the Fabric Manager window.

Note: The icon that displays the **View Selector** () serves other functions when it is displayed in other locations. Only the icon in the top right corner of the interface displays the view selector.

The view selector is displayed. [Figure 3](#) shows the View Selector bar with all of the views available for a switch.



Figure 3: View Selector Bar

2. Click the view that you want to access.

For more information on the views, see [Appendix C](#).

[Table 3](#) describes the views available in Fabric Manager.

Table 3: Fabric Manager Views

View	Description
Overview View	Provides information about the components and status of an element. An At-A-Glance window is displayed for each element in this view, depending on what you have selected from the SAN Elements tab.
Alerts View	Provides alerts that you have configured to be notified about.
Topology View	Provides a graphical display of fabric topology.
Switches View	Provides information about the status and traits of each switch.
Devices View	Provides information about all devices that connect to an element.
Device Ports View	Provides a list of device ports attached to a given element in the SAN Elements tab.
Ports View	Provides detailed information about the ports.
Portgrid View	Displays the node that connects to each port. The Portgrid View displays devices only; it does not show Intersite Link (ISL) information.
LSAN View	Provides information about LSAN zones in the fabric.
Events View	Provides an event log for the element and the status reason.
LSAN Info View	Provides information about MP Routers in the 3 sub-views: Physical Devices, Proxy Devices, and LSAN Info.

ID Menu

The ID Menu allows you to customize how you view your switches and fabrics. For instructions on selecting identities with the **ID** field, see [“Displaying SAN Elements by IP address, Domain ID, WWN, and Name”](#) on page 50.

SAN Elements Tab

The **SAN Elements** tab displays the various elements that you monitor with Fabric Manager. As you use Fabric Manager, you repeatedly select items from the **SAN Elements** tab to configure and monitor.

When an element that Fabric Manager monitors changes physical status, the background of element's icon changes color in the **SAN Elements** tab, as do the background colors of the parent element icons. The background color of the element icons in the **SAN Elements** tab for each element indicates the physical status of that element, where:

- Green indicates the element is healthy
- Yellow indicates the element is marginal
- Red indicates the element is critical
- Gray indicates the element is unknown or unmonitored

Note: Port status does not affect switch icon background color. When the background of an element in your **SAN Elements** tab changes color, the change does not necessarily represent the failure of an entire fabric or switch. Expand the navigation tree to identify the source of the status change.

Filter Tab

The **Filter** tab lets you view elements that include a particular alphanumeric string. For instance, if you name all switches for your Accounting team acctx, where x is a number, you can view just your accounting switches. If you select **name** from the menu, type acct in the text field, and click **Enter**. The **Filter** tab displays every switch that has acct in its name. For more information on how to filter elements, see “[Filtering Elements](#)” on page 54.

You can filter elements by the following attributes:

- IP address
- Name
- Switch Type
- Version
- WWN (World Wide Name)
- Domain ID

Storing Data

You must log in to the Fabric Manager software. Fabric Manager stores the following user settings locally (on the client machine):

- Fabric Manager user name
- Host name/server IP address of all servers you have successfully accessed
- Browser path to launch Advanced Web Tools
- Dimensions of the Fabric Manager window

The following user settings are served on the database in the server:

- Group definitions
- Discovered fabrics
- User interface settings (view customizations, topology locations, and so on)
- Switch user names and passwords

Other settings are global to all clients running on the same Fabric Manager server.

Fabric Manager stores user settings when you exit, not while you run the software. When the client attempts to log in to the server, the server authenticates the client login. After the server authenticates the client, Fabric Manager launches and polls switches.

Persistent Files

[Table 4](#) describes the files that store user settings.

Note: In Fabric Manager 4.0 and 4.1.0, information was stored differently than in Fabric Manager 4.2.x.

Table 4: Fabric Manager 4.2.x Persistent Files

File	Location	Contents
FabricManager.properties	client	Stores Fabric Manager host name/IP addresses and ports, user name, browser path, Fabric Manager window dimensions, and x and y coordinates.
LocationTable	server	Stores x and y locations for topology nodes in Topology View.
FabricManagerUser.properties	server	Stores user interface settings such as known fabrics, file transfer settings, and default layout and link styles for the Topology View.
SwitchInfo.txt	server	Stores switch login information with passwords encrypted.

System Requirements

For some Fabric Manager functions to function correctly, TCP/UDP port numbers 20, 21, 111 (rpc mapping) and 600-1023 must not be blocked by a network firewall or proxy server or secure Fabric OS policy for HTTP or API.

You must enable HTTP protocol on every switch that you want to discover, monitor, and configure with Fabric Manager. You must also enable HTTP on your SAN. For instructions on enabling HTTP on switches, refer to the *HP StorageWorks Fabric OS 4.2.x Procedures User Guide* and the *HP StorageWorks XPath OS Version 7.1.x Procedures User Guide*.

Client and Server Machines

This section discusses client and server machines in the Windows[®] and Solaris environments.

Windows Environments

For a fabric with 1-500 ports or 1- 20 switches, it is recommended that your machines have the following if you are running client and server separately:

- Client: An 800 MHz CPU with a minimum of 256 MB memory
- Server: A 1.8 GHz P4 with 512 MB memory

With this size fabric, Fabric Manager Client and Server should be running on the same machine, so you should meet the server requirements if you are running them on the same machine.

For a fabric with 500 -1500 ports or 21-50 switches, it is recommended that your machines have the following if running client and server separately:

- Client: A1.5 GHz CPU with a minimum of 512 MB memory.
- Server: A 2.0 GHz P4 CPU with a minimum of 768 MB memory.

With this size fabric, Fabric Manager Client and Server should be running on the same machine, so you should meet the server requirements if you are running them on the same machine.

For a fabric with 1501 to 2300 ports or 51-80 switches, it is recommended that your machines have the following if running client and server separately:

- Client: A1.5 GHz CPU with a minimum of 512 MB memory.
- Server: A 2.5 GHz P4 CPU with a minimum of 1GB memory.

With this size fabric, Fabric Manager server should be running on a separate machine.

Solaris Environments

For a fabric with 1-500 ports or 1- 20 switches, it is recommended that your machines have the following if running client and server separately:

- Client: An Ultra 5 300 MHz CPU with a minimum of 256 MB memory.
- Server: An Ultra 10 400 MHz CPU with 512 MB memory.

With this size fabric, Fabric Manager Client and Server should be running on the same machine, so you should meet the server requirements if you are running them on the same machine.

For a fabric with 500 -1500 ports or 21-50 switches, it is recommended that your machines have the following if running client and server separately:

- Client: An Ultra 10 400 MHz CPU with a minimum of 512 MB memory.
- Server: An Ultra 60 450 MHz CPU with a minimum of 1 GB memory.

With this size fabric, Fabric Manager Client and Server should be running on the same machine, so you should meet the server requirements if you are running them on the same machine.

For a fabric with 1501 to 2300 ports or 51-80 switches, it is recommended that your machines have the following if running client and server separately:

- Client: An Ultra 30 400 MHz CPU with a minimum of 768 MB memory.
- Server: An Ultra 60 450 MHz CPU with a minimum of 2 GB memory.

With this size fabric, Fabric Manager server should be running on a separate machine.

Supported Devices

Fabric Manager 4.2.x supports many different devices. For a detailed list of which devices are supported running which versions of firmware, refer to the *HP StorageWorks Fabric Manager Version 4.2.x Release Notes*.

Supported Operating Systems

Fabric Manager Client and server run on Windows and Solaris operating systems. The list of supported operating systems is not the same for the client and server, so if you are running client and server on different machines, check the list in the next section to ensure that the operating system is supported for the client or server.

Fabric Manager Client

The Fabric Manager client accesses switches under management through an Ethernet connection. If your client and server are on different machines, you must ensure that both machines (client and server) have access to the switches.

Fabric Manager client runs on the following operating systems:

- Windows 2000
- Windows 2003

- Windows NT[®] 4.0
- Windows XP[®]
- Solaris 2.7
- Solaris 2.8
- Solaris 2.9

Note: Advanced Web Tools requires Java[™] Plug-in version 1.4.2_03.

Fabric Manager Server

Fabric Manager server runs on the following operating systems:

- Windows 2000
- Windows 2003
- Windows XP
- Solaris 2.8
- Solaris 2.9

Each Fabric Manager server can support up to five Fabric Manager clients.

Firmware Specific Features

For a detailed list of firmware and hardware supported by Fabric Manager, refer to the *HP StorageWorks Fabric Manager Version 4.2.x Release Notes*.

Some Fabric Manager features run only on particular firmware versions. [Table 5](#) lists the features that run only on particular versions and the versions on which they run.

Table 5: Firmware-Specific Features

Feature	Firmware Versions
Port name change on a switch	Fabric OS v3.1.0 and later Fabric OS v4.1.0 and later XPath OS v7.1.0 and later
Topology/ISL monitoring	Fabric OS v2.6.0k and later Fabric OS v3.02k and later Fabric OS v4.0, 4.1.0 and later
Security	Fabric OS v2.6.x Fabric OS v3.1.0 and later Fabric OS v4.1.0 and later
Port swapping	Fabric OS v4.1.0 and later
FDML/ HBA firmware download	Fabric OS v3.1.0 and later Fabric OS v4.1.0 and later
Performance monitoring	Fabric OS v4.2.0c and later ¹
QuickLoop	Fabric OS v2.x Fabric OS v3.x ²

Table 5: Firmware-Specific Features (Continued)

Feature	Firmware Versions
Multi-protocol Router	XPath OS v7.1.x
<p>Change Management configuration checking: The Fabric Manager server uses API libraries to get switch configuration and security policy information from switches.</p> <p>If a fabric has a switch running firmware versions 2.6.x or earlier, or 3.0 or earlier, or XPath OS v7.1.0, Change Management switch configuration checking is not supported.</p> <p>Fabric Manager uses one switch in the fabric to collect security policy information through API. Fabric Manager cannot collect security policy information for a fabric if the switch it selects is running firmware versions 2.6.x or earlier, or 3.0 or earlier, or XPath OS v7.1.0, because API does not support those versions of firmware or that switch type.</p>	<p>Fabric OS v2.6.x and later</p> <p>Fabric OS v3.1.0 and later</p>
SupportShow information in Fabric Manager	<p>Fabric OS v3.1.0 and later</p> <p>Fabric OS v4.1.0 and later</p>

1. Performance Monitoring port stats return incorrect values for all versions of 4.x to 4.2.0b. Firmware versions later than 4.2.0c work correctly.
2. The QuickLoop feature can be implemented only on switches running 2.x or 3.x firmware versions, however, when using a launch switch running 4.x firmware, you can see the 2.x and 3.x switches in QuickLoops.

Installing and Upgrading

2

This chapter describes how to install the Fabric Manager client and server software on the supported operating systems. Choose from the following types of installation:

- “[Full Version](#)” on page 32
- “[Evaluation Version](#)” on page 32

Fabric Manager gives you the option of installing the following:

- Fabric Manager Server and Client
- Fabric Manager Server only
- Fabric Manager Client only

Installing Fabric Manager

When you install Fabric Manager over an existing version on a Windows system, the installer finds the existing serial number and license key and attempt to validate them. If the serial number and license key are valid, the installer skips the version selection panel and go directly to the install set panel. The serial number and license key are saved. If the serial number and license key are not valid, you must re-enter the serial number and license key to install the full version of Fabric Manager.

When you install Fabric Manager over an existing version on a UNIX[®] system, the installer prompts you to select the location where the existing version of Fabric Manager is installed. Then the installer finds the existing serial number and license key, and attempt to validate them. If the serial number and license key are valid, the installer skips the version selection panel and go directly to the install set panel. The serial number and license key are saved. If the serial number and license key are not valid, you must re-enter the serial number and license key to install the full version of Fabric Manager.

Full Version

A valid serial number and license key are required for a full installation.

Evaluation Version

Fabric Manager offers an evaluation version that you can use for up to 60 days. You do not need to provide a serial number or license key to use the evaluation version; however, you must accept the license agreement displayed during the installation.

Every time you launch Fabric Manager, a warning message is displayed, notifying you when the evaluation version expires and giving you the option to register Fabric Manager or continue with the evaluation version (see [Figure 4](#)).

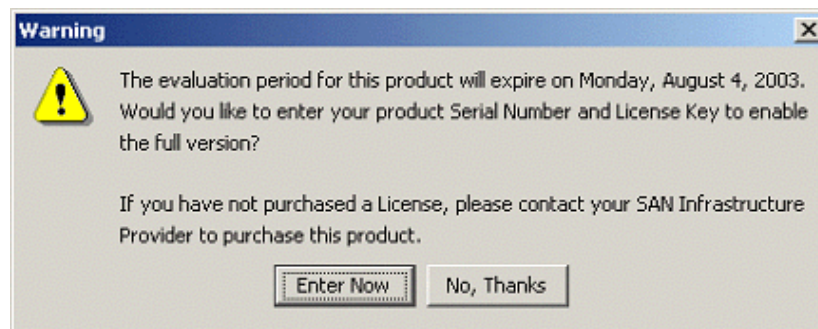


Figure 4: Fabric Manager Evaluation Installation Version Warning

After the sixtieth day, the evaluation version expires and an error message is displayed when you launch the evaluation version of Fabric Manager (see [Figure 5](#)).

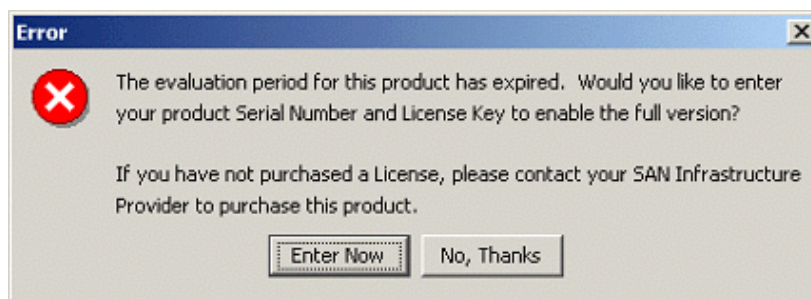


Figure 5: Fabric Manager Evaluation Installation Version Expiration Error

You have the option of registering the software to make it a full version or discontinue use of Fabric Manager.

Any time before the 60 days are up, you can convert your evaluation version to a full version by registering Fabric Manager. You can register Fabric Manager in any of the following ways:

- Click **Enter Now** from the warning message that is displayed when you launch Fabric Manager every time during the 60 day evaluation period (see [Figure 4](#)). Enter your serial number and license key.
- Click **Enter Now** from the error message that is displayed when you launch Fabric Manager after the 60 day evaluation period is up (see [Figure 5](#)). Enter your serial number and license key.
- Select **Register** from the **Help** menu in Fabric Manager. For detailed instructions, see “[Registering Fabric Manager](#)” on page 40.

After launching the Fabric Manager installer on Windows XP or 2003 machine, if an After Installation window is displayed, click **Cancel** to exit that program. The Fabric Manager is a Windows program and exists only on some Windows XP or 2003 machines depending on your Windows image.

If you do not cancel it, it moves your Fabric Manager shortcut to the All Users folder after the Fabric Manager installation is complete. Later, when you uninstall Fabric Manager, the uninstaller is not able to remove the Fabric Manager menu item from the **Start > Programs** menu. If you install only the Fabric Manager server, it does not cause any problems. If you install the client or both the client and server, this problem does occur.

Installing the Client and Server Together or Installing Server Only

In a Windows environment, if the server workstation is not a member of the domain specified during installation, Fabric Manager authentication succeeds for *any* user credentials (if the guest account on the workstation is enabled).

After launching the Fabric Manager 4.2.x installer on a Windows XP or 2003 machine, if you see another After Installation window, click **Cancel** to exit that program. The Fabric Manager installer is a Windows program that exists only on some Windows XP or Windows 2003 machines, depending on your Windows image.

If you do not cancel it, your Fabric Manager shortcut is moved to the All Users folder after the installation is complete. When you uninstall Fabric Manager, the uninstaller is not able to remove the Fabric Manager menu item from the **Start > Programs** menu.

To ensure that the security of your Fabric Manager Server is not compromised, ensure that your Windows guest user permissions are disabled and that your Fabric Manager server workstation is a member of the domain you specify during the Fabric Manager server installation. For instructions on disabling your Windows guest user permissions, refer to your Windows documentation.

To install the Fabric Manager server and client at the same time:

1. For Windows: Double-click the **Windows** folder from the Fabric Manager Installation CD-ROM.

For Solaris: Click `install.bin` from the File Manager window that is displayed when you insert the Fabric Manager Installation CD-ROM.

2. Double-click the **Install** icon. The InstallAnywhere dialog box runs and the Fabric Manager installation wizard is displayed.
3. Click the version you would like to install (Evaluation or Full) and then click **Next**. A valid serial number and license key are required for a full installation. You cannot continue the full installation process without a valid serial number and license key.
4. Enter a valid serial number and license key and then click **Next**. You are prompted to wait while Fabric Manager configures your system. The Choose Install Set screen is displayed.
5. Click the **Server and Client** icon. The selected Install Set text turns blue.
6. Click **Next**.

If you have a Fabric Manager server (or server and client) version earlier than Fabric Manager 4.2.x installed, a message is displayed warning you that you can lose all information in the database if you proceed with the installation of the new server. You should make a copy of your database if you want to retain your existing information. To back up the database, select a backup folder. Select the configuration you want to back up. The Fabric Manager installer migrates the previous server configuration to the new server database.

If you have a Fabric Manager client version earlier than Fabric Manager 4.2.x installed, the Fabric Manager installer uninstalls the old Fabric Manager client installation before installing the 4.2.x installation.

7. Click **Next**. If you do not currently have a version of Fabric Manager server installed, the Introduction screen is displayed.
8. Read the introduction and click **Next**. The Select Destination Folder screen is displayed. The default destination location is `C:\Fabric Manager`.
9. Optional: If you want to change the default location, click **Choose**. The Browse for folder window is displayed. Select a new location and click **OK** in the Browser for folder. You can also enter a new destination folder, but the path should not contain spaces. For Solaris workstations, the folder name cannot exceed 59 characters.

10. Click **Install**. You are prompted to wait while Fabric Manager is installed on your system. The Please Specify Starting Port Number screen is displayed.

The default starting port number is 24600. The port number you enter and the next five ports must be free ports. If the default starting port number is not a free port number, the server cannot start up correctly.

11. Optional: You can enter a new port number if all six ports (the port number you enter, and the next five ports) are free ports. Make note of the port number you enter. When you install clients to access this server, you must use the same port number during the client installation.

12. Click **Next**. You are prompted to wait while Fabric Manager configures your system.

For Windows: The Windows domain/work group name screen is displayed.

For Solaris: You are prompted to select an authentication method: NIS authentication or Password file authentication.

13. Select one of these and then click **Next**.

14. For Windows: Enter the windows domain or work group name and then click **Next**.

For Solaris: If you selected Network Information Service (NIS) authentication, enter your hostname/IP address and NIS domain name. If you selected Password file authentication, click **Next** without entering any information. The Important Information screen is displayed.

15. Read the information and then click **Next**. You are prompted to wait while the Fabric Manager server is started. This might take a few minutes. The Configure Client Options screen is displayed.

16. For Windows: Enter the Fabric Manager Server IP address.

Note: In a Windows environment, if the server workstation is not a member of the specified domain, Fabric Manager authentication succeeds for any user credentials (if the guest account on the workstation is enabled).

To ensure that the security of your Fabric Manager Server is not compromised, disable your Windows guest user permissions and ensure that your Fabric Manager server workstation is a member of the domain you specify during the Fabric Manager server installation. For instructions on disabling your Windows guest user permissions, refer to your Windows documentation.

For Solaris: Enter your NIS hostname or IP address and domain name for the Fabric Manager server user authentication. If you do not specify an NIS server host name or IP address, and no NIS server exists on the same subnet as the Fabric Manager server, all authentication requests to that server fail.

Valid domain names:

- Include no more than 67 characters (including .com, .net, .org at the end).
- Include only alphanumeric characters and hyphens (-); spaces and other characters are not permitted.
- Cannot begin or end with a hyphen (-).

17. Click **Next**. The Install Complete screen is displayed.

18. Optional: You can click the **View Readme** check box to open the Readme file after exiting the Installation wizard.

19. Click **Done** to exit the Installation wizard.

Installing Fabric Manager Client Only

If you are installing the Fabric Manager Client over an existing installation of the Fabric Manager Client (without uninstalling the old version first), you must manually edit the system path to include only one Fabric Manager client directory. The Fabric Manager installer launches the uninstaller of the previous Fabric Manager client and uninstalls it before installing the Fabric Manager 4.2.x client.

After launching the Fabric Manager 4.2.x installer on a Windows XP or 2003 machine, if you see another After Installation window, click **Cancel** to exit that program. The Fabric Manager installer is a Windows program that exists only on some Windows XP or 2003 machines depending on your Windows image.

If you do not cancel it, your Fabric Manager shortcut is moved to the `All Users` folder after the installation is complete. When you uninstall Fabric Manager, the uninstaller is not able to remove the Fabric Manager menu item from the **Start > Programs** menu.

The installation wizard does not check to see if there is an existing path specified for the Fabric Manager Client during the installation, and just appends to the system path file, resulting in multiple paths. Although multiple paths do not affect functionality, they could result in other applications being unable to add additional path names, since Fabric Manager Client paths are too lengthy.

To install the Fabric Manager client:

1. For Windows: Double-click the `Windows` folder from the Fabric Manager Installation CD-ROM.

For Solaris: Click `install.bin` from the File Manager window that is displayed when you insert the Fabric Manager Installation CD-ROM.

2. Double-click the **Install** icon. The InstallAnywhere dialog box runs and the Fabric Manager installation wizard is displayed.
3. Click the version you would like to install (Evaluation or Full) and then click **Next**. A valid serial number and license key are required for a full installation. You cannot continue the full installation process without a valid serial number and license key.
4. Enter a valid serial number and license key and then click **Next**. You are prompted to wait while Fabric Manager configures your system. The Choose Install Set screen is displayed.
5. Click the **Server and Client** icon. The selected Install Set text turns blue.
6. Click **Next**.

If you have a Fabric Manager server (or server and client) version earlier than 4.2.x installed, a message is displayed warning you that you can lose all information in the database if you proceed with the installation of the new server. Make a copy of your database if you want to retain your existing information. To back up your database, select the backup folder. Fabric manager backs up the previous Fabric Manager server configuration and then uninstalls the previous server.

If you have a Fabric Manager client version earlier than 4.2.x installed, Fabric Manager uninstalls the previous version of Fabric Manager before installing the Fabric Manager 4.2.x client.

7. Click **Next**. If you do not currently have a version of Fabric Manager server installed, the Introduction screen is displayed.
8. Read the introduction and click **Next**. The Select Destination Folder screen is displayed. The default destination location is `C:\Fabric Manager`.

9. Optional: If you want to change the default location, click **Choose**. The Browse for folder window is displayed. Select a new location, and click **OK** in the Browse for folder. You can also enter a new destination folder, but the path should not contain spaces. For Solaris workstations, the folder name cannot exceed 59 characters.
10. Click **Install**. You are prompted to wait while Fabric Manager is installed on your system.
11. The Configure Client Options screen is displayed.
12. Enter your server IP address and a server port number. The server IP address you enter is the default server for the Fabric Manager client. The server port number must be the same port number as the starting port number of the Fabric Manager Server.
13. Click **Next**. The Install Complete screen is displayed and the installation is complete.
14. For Solaris, log out of your workstation and log in again to access all Fabric Manager features.

Upgrading Fabric Manager

If you are upgrading to a newer version of Fabric Manager, see [Table 6](#) for the supported upgrade paths and the level of license and configuration information stored on the server through the upgrade.

Table 6: Upgrading Fabric Manager From a Previous Version

	FM 3.0.2c	FM 4.0	FM 4.0.1	FM 4.1.0	FM 4.1.1	FM 4.2.x
FM 3.0.2c						
license	NA	No	No	No	No	No
configs	NA	Information from the FabricManager.xml and FabricManager.Properties file	Information from the FabricManager.xml and FabricManager.Properties file	Information from the FabricManager.xml and FabricManager.Properties file	Information from the FabricManager.xml and FabricManager.Properties file	Information from the FabricManager.xml and FabricManager.Properties file
FM 4.0						
license	NA	NA	No	The license is retained if you have FM 4.0 client (or client and server) installed.	The license is retained if you have FM 4.0 client (or client and server) installed.	
configs	NA	NA	No	Yes	Yes	
FM 4.0.1						
license	NA	NA	NA	The license is retained if you have FM 4.0 client (or client and server) installed.	The license is retained if you have FM 4.0 client (or client and server) installed.	
configs	NA	NA	NA	Yes	Yes	
FM 4.1.0						
license	NA	NA	NA	NA	The license is retained if you have FM 4.0 client (or client and server) installed.	
configs	NA	NA	NA	NA	Yes	
FM 4.1.1						
license	NA	NA	NA	NA	NA	
configs	NA	NA	NA	NA	NA	
FM 4.2.x						
license	NA	NA	NA	NA	NA	
configs	NA	NA	NA	NA	NA	

Note: If you currently have only Fabric Manager Server v4.0.x (or earlier) installed and you are upgrading to Fabric Manager v4.1.0 (server only, client only, or server and client) or later, the installer prompts you to reenter the license key and serial number.

If you are upgrading from Fabric Manager 3.0.x directly to Fabric Manager 4.2.x, you need a new license key.

Fabric Manager versions earlier than 4.2.x allowed user-level settings, which were stored on the client machine. Starting with Fabric Manager 4.2.x, fabric, switch, and port settings are global for all users sharing the same Fabric Manager server. When you upgrade to Fabric Manager 4.2.x or later, you can select one user's old fabric and group settings to migrate to the server for all users (of that server) to use. All information previously stored in the `FabricManagerUser.properties` and `SystemInfo.txt` files is migrated to the new version of Fabric Manager. These files include:

- Fabrics, switch, port, and group-level details, such as names and descriptions as defined for one specified user during the Fabric Manager 4.2.x installation
- Switch login state and passwords, as defined for one specified user during the Fabric Manager 4.2.x installation

The following information cannot be migrated to Fabric Manager 4.2.x and must be reset by any user on the server:

- Topology settings
- View customization
- At-A-Glance window customization

Launching Fabric Manager for the First Time

To launch Fabric Manager for the first time, perform the following steps:

1. For Windows: From the **Start** menu, select **Programs > Fabric Manager > Fabric Manager**.

For Solaris: Navigate to the location where you installed Fabric Manager. Run the `startFabricManager` script.

The Fabric Manager Login dialog box opens. Fabric Manager automatically populates the Server and Port fields of the dialog box with the values that you specified when you installed the application.

2. In the **User name** field, enter the user name that you use to log in to the server.

Note: Fabric Manager stores your user name and automatically populates this field when you subsequently launch the software. User names must be alphanumeric; the only special characters they may contain are underscore (`_`), dashes (`-`), and periods (`.`).

3. In the **Password** field, enter the password that you use to log in to the server and click **OK**. Fabric Manager launches.

Registering Fabric Manager

During a full installation, Fabric Manager is automatically registered. If you install the evaluation version of Fabric Manager, you need to register Fabric Manager within 60 days of the installation. After 60 days, the evaluation version is not usable until it is registered; registration changes it into a full version.

To register Fabric Manager using the Fabric Manager GUI:

1. Select **Register** from the **Help** menu. The Fabric Manager Registration window is displayed.
2. Enter a valid serial number and license key.
3. Click **Enter**. A Congratulations dialog box opens, indicating that you have successfully registered Fabric Manager.
4. Click **OK** in the Congratulations dialog box.
5. Click **Cancel** to close the Fabric Manager Registration window.

Uninstalling Fabric Manager

To uninstroll Fabric Manager, follow the procedures in this section.

Windows Operating Systems

To uninstall Fabric Manager under Windows:

1. From the **Start** menu, select **Programs > Fabric Manager > Uninstall Fabric Manager**.
2. Click **Next**.
3. Click the **Complete Uninstall** icon to remove both the Fabric Manager client and server from your machine, or click the **Uninstall Specific Features** icon and proceed as follows:
 - a. Click **Next**.
 - b. Uncheck features that you want to uninstall.
 - c. Click **Uninstall**.
4. Click **Done**.

Solaris Operating Systems

To uninstall Fabric Manager under Solaris:

1. Navigate to the location where you installed Fabric Manager.
2. From the `Fabric_Manager/ UninstallerData` directory, run `Uninstall_FabricManager`.
3. Click **Next**.
4. Click the **Complete Uninstall** icon and click **Next**.
5. Click **Done**.

Fabric Management

3

Discovering a Fabric

You must *discover* a fabric to add it to the SAN Elements tab and administer it with Fabric Manager.

To discover a fabric:

1. Place your cursor in the Address field and delete the contents of the field.
2. Enter the IP address or the DNS name of a switch in the fabric that you want to administer and press **Enter**. You do not need to include `http://` before the IP address to discover a fabric.

Running a Subnet Scan (Fabric Scan)

Fabric Manager can scan a subnet to discover fabrics. With this discovery mechanism, you do not need to know the exact address of a switch to discover a fabric. When you specify a subnet, Fabric Manager lists the switches and fabrics that it finds so that you can add them to the SAN Elements tab.

Note: Switches might appear in your subnet scan even after you unplug the Ethernet cables of those switches.

To run a subnet scan:

1. Select **Tools > Subnet scan**. The Subnet scan dialog box opens.
2. Enter the first three sets of digits of an IP address in the first three sections of the **IP Address Range** field.
3. Enter a wildcard in the last section of the **IP Address Range** field to represent the range of scan. Choose from one of the following three options:
 - **192.168.168.*** discovers any fabric in the address range of 192.168.168.0–192.168.168.255.
 - **192.168.168.1**** discovers any fabric in the address range of 192.168.168.100–192.168.168.199. (The first digit in the wildcard cannot exceed a value of 2; see Note.)
 - **192.168.168.11*** discovers any fabric in the address range of 192.168.168.110–192.168.168.119. (See Note.)

Note: The number before the asterisk (*) can be any number, as long as the resulting range is greater than 0 and less than 255. For example, you cannot enter 192.168.168.3** or 192.168.168.26*. Also, if you enter 192.168.168.25*, the range is 192.168.168.250–192.168.168.255.

4. Click **Scan**. The scan result is displayed. IP addresses that appear as underlined links with two angle brackets (>>) represent fabrics.
5. Click the link to view the switches in the fabric.

Note: To add a switch or fabric to your SAN Elements tab, click the check box next to the element and then click **Add**.

Deleting a Fabric

When you delete a fabric, any change management profiles and snapshots are deleted; Performance Monitoring data is removed (this includes historical statistics for the switches currently in the fabric and any reports and graphs that have been generated and saved back to the database of the deleted fabric). Any switches and ports within the fabric are also removed from any switch or port groups they were members of.

To stop monitoring a fabric with Fabric Manager, perform the following steps:

1. Click the fabric from the SAN Elements tab that you want to remove from Fabric Manager.
2. Select **Actions > Delete** to remove the fabric. Fabric Manager prompts you to make sure that you want to delete the fabric.

Renaming a Fabric

When you discover a fabric, Fabric Manager assigns a name to that fabric that matches the name of the switch that you used to discover the fabric. For instance, to monitor a fabric that includes Switch_01, enter the IP address of Switch_01 in the Address field to discover the fabric. Fabric Manager then names that fabric Switch_01 and displays that name in the SAN Elements tab.

After you discover the fabric, you can assign a name to the fabric that is more meaningful to you (for instance, mktng_SAN or HQ).

Fabric information is global and any changes you make to the fabric, including renaming the fabric, are displayed to all users connected to the server.

To rename a fabric:

1. In the SAN Elements tab, click the fabric that you want to rename.
2. From the **Edit** menu, select **Rename**. A cursor is displayed to the right of the current name. You can also use the **F2** key or triple-click a fabric, switch, or port icon to rename it.
3. Rename the fabric and press **Enter**. You can also triple-click a fabric, switch, or port icon to rename it. In Windows, you can also press **F2**.

Renaming a Switch

Switch information is global and any changes you make to the switch, including renaming the switch, are displayed to all users connected to the server.

To rename a switch:

1. In the SAN Elements tab, click the switch that you want to rename. You must be logged in to that switch. If you are not logged in to the switch, Fabric Manager prompts you to log in before proceeding.
2. Select **Edit > Rename**. A cursor is displayed next to the name of the switch in the SAN Elements tab.
3. Enter a new name for the switch and press **Enter**. You can also triple-click a fabric, switch, or port icon to rename it. In Windows, you can also press **F2**.

Renaming a Port

When you rename a port on a switch that runs firmware versions earlier than 3.1.0 or 4.1.0, the port name is local to each Fabric Manager client, and must be changed individually on each client.

If you rename a port on a switch that runs firmware versions 3.1.0 (and later) or 4.1.0 (and later), Fabric Manager propagates that name to the port and changes the port name on the switch, provided the fabric login information has been set up successfully.

Port information is global and any changes you make to the port, including renaming the port, are displayed to all users connected to the server.

To rename a port:

1. Click the port that you want to rename from the SAN Elements tab.
2. Select **Edit > Rename**. A cursor is displayed next to the name of the port in the SAN Elements tab.
3. Enter a new name for the port and press **Enter**. You can also triple-click a fabric, switch or port icon to rename it. In Windows, you can also press **F2**.

Renaming a Device Node and Device Port

Device nodes and device ports are identified using WWN and SCSI inquiry or symbolic names. You can name devices using zone aliases by placing a WWN in a zone alias and then specifying the name. The device is then identified by the name of the alias where the device is placed, using the zone alias as the name of the device.

Fabric Manager allows you to import names for devices from the zone aliases defined in the zoning database on a fabric. You can also rename the devices manually. The devices are then identified by the new name attribute wherever they are displayed in Fabric Manager screens (for example, in the Share Device wizard, LSANs display, device port table, device node table).

You can edit device node and device port names from the device node and device port tables (see [Figure 6](#)) or from the At-A-Glance view for the device.

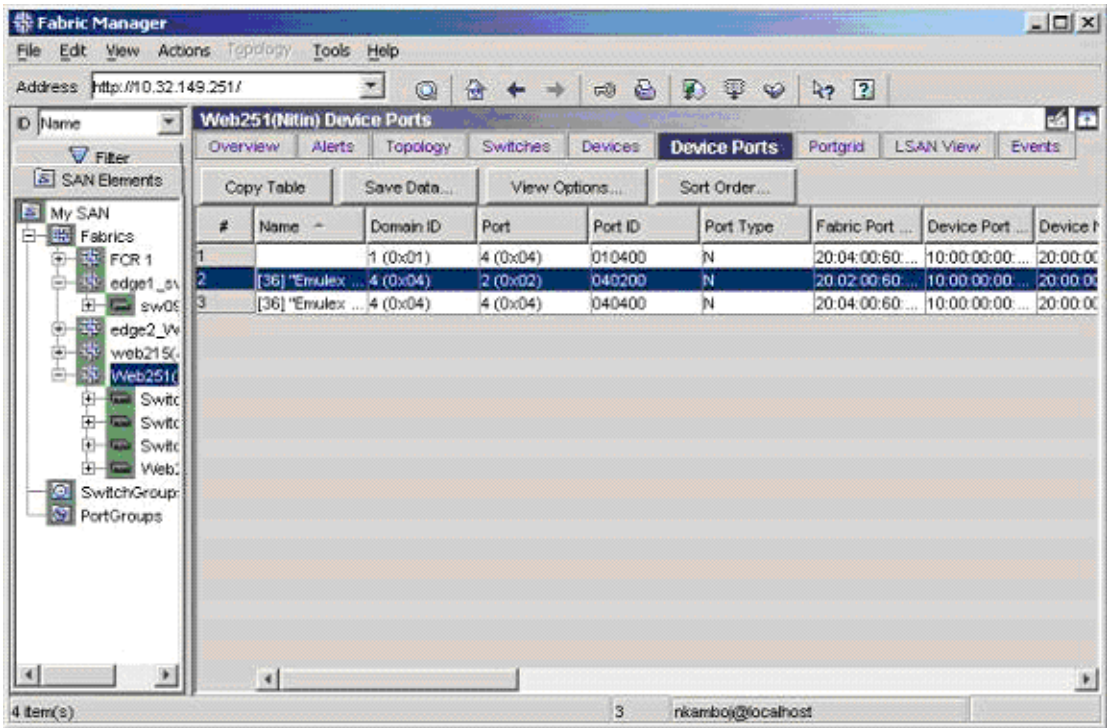


Figure 6: Device Ports Screen

Select a row within the Device Ports window, then right-click to rename the selected device port (see Figure 7).

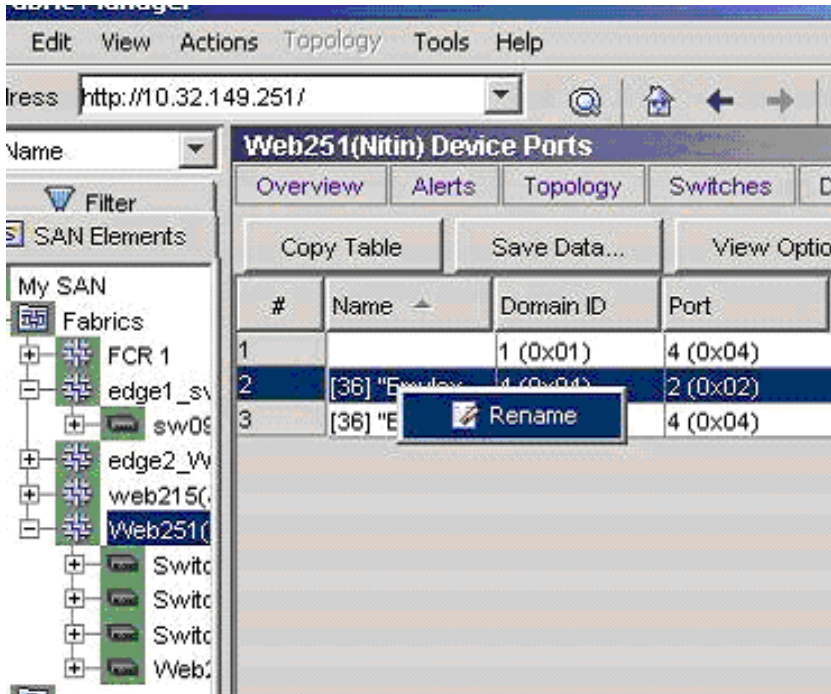


Figure 7: Renaming a Device Port

You can also import the names from aliases defined in the zoning database of fabrics via a **Tools** menu option. From the Tools menu, select the **Import Device Node/Port Names** option (see [Figure 8](#)).

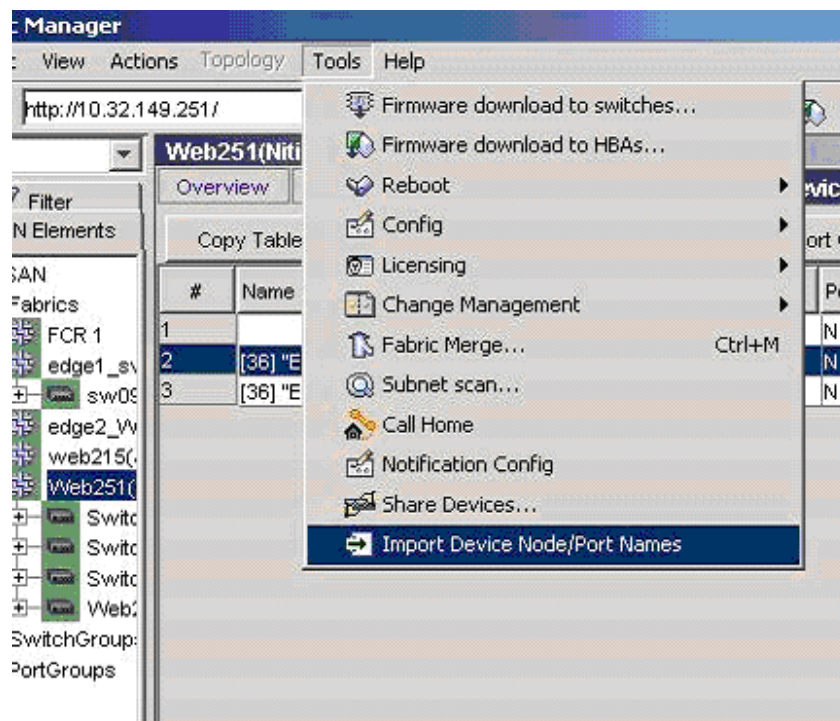


Figure 8: Importing Alias Names

If an alias contains more than one member, the alias is ignored. If a WWN is contained in more than one alias, one of the aliases is picked at random to set the name. An import operation overrides current names for devices.





The names are global to the instance of the Fabric Manager server and they apply to the Device Node and Device Ports for all fabrics on that Fabric Manager server. The name value is stored in a different table than the Device Node and Device Port information, so that even if the device leaves the fabric and returns, the user-configured name is not lost. The name defaults to `SCSI inquiry name` for device nodes and `symbolic name` for device ports.

Customizing a View

Customize a view so that each time you select that view, it displays only the information that you want to see in the order you have selected. You can also sort the order of the columns, and sort the order of information displayed in the columns. In addition, you can perform multi-column sorts, where you can specify the order in which the information in the columns is sorted (it sorts the information in one column and then another column, and so on).

To customize the contents displayed in a view and the order of the columns displayed:



1. Click any element from the SAN Elements tab.
2. Select **View > View Type**, where *View Type* is the view that you want to customize.
3. Select **Edit > View Options**. You can also click the **View Options** button in the view (except in Topology view and Overview view). The Edit View Options dialog box opens.

4. Optional: To customize what information is displayed (which columns in all tables views, not the Overview view or Topology view) in the selected view, click an item in the **Available Items** list and then click the right arrow icon  to add items to the **Display Items** list, or the left arrow icon  to remove items from the **Display Items** list. You can press the **Ctrl** and **Shift** keys to select multiple items at once.
5. Optional: You can customize the order of the information displayed as ascending or descending in all table views (not the Overview view or Topology view). You can also rearrange the order of columns by clicking an item from the **Display Items** list and then clicking the up  or down  arrow icons.
6. Click **OK**.

To customize the sorting of the information displayed in a view:

1. Click any element from the SAN Elements tab.
2. Select **View > View Type**, where *View Type* is the view (except Topology view and Overview view) in which you want to sort information.
3. Optional: To sort the order of contents in a column as ascending or descending, click the header of that column. Each time you click the column header, the order toggles between ascending and descending.
4. Optional: You can also sort the order of contents in a column as ascending or descending by clicking the **Sort Order** button in the view (except in Topology view, Portgrid view, and Overview view).

The Edit Sort Order dialog box opens. In this dialog box, you can also sort the order of contents in a column as ascending or descending.

- a. To sort the order of a column's contents as ascending or descending, click the column header that you want to sort from the **Available Items** list and then click the right arrow icon to add items to the **Display Items** list. Once an item is in the **Display Items** list, you can arrange the order of contents. Click the ascending icon  to sort the items in that column in an ascending order. Click the descending icon  to sort the items in that column in a descending order.
- b. To rearrange the order in which the columns are sorted, click an item from the **Display Items** list and then click the up or down arrow icons. The first item in the list is sorted first, then the second item, then the third, and so on.
- c. Click **Apply**.
- d. Click **OK**.

Disabling Table View Tooltips

Fabric Manager views that display information in table format also display tooltips of the entire text of the cell when you move the mouse over the cell. This is useful in tables where a lot of information is displayed and you must expand a column to see all of the information. You can mouse over the cell to display the entire contents of the cell in a tooltip. These table view tooltips are enabled by default, but you can disable them.

To disable table view tooltips:

1. Select **File > Options**. The Options dialog box opens.
2. To disable the table view tooltips, click **Show Table Tooltips** (so that the check mark disappears).
3. Click **OK**.

Copying Fabric Manager View Information to Spreadsheet Applications

Fabric Manager views display information in table format (except Overview view and Topology view). Those tables can be copied to spreadsheet applications.


To copy a table to a spreadsheet application:

1. Click any element from the SAN Elements tab.
2. Select **View > View Type**, where *View Type* is any view that displays tables (except Overview View or Topology View).
3. Click **Copy Table**. You can also select **Edit > Copy Table**. A confirmation message is displayed, indicating that the information is copied to the clipboard.
4. Click **OK** in the confirmation message.
5. Open a spreadsheet application.
6. In the spreadsheet application, open a new spreadsheet and paste the information.

Printing Fabric Manager View Information

Fabric Manager can print the contents of all views except the Overview View.

To print the information displayed in a Fabric Manager view:

1. Select **View > View Type**, where *View Type* is any view except the Overview View.
2. Select **File > Print**, or click the **Print** icon  to print. From the Topology View only, you can also select **File > Print In One Page** to print all of the topology information on one page. The Print dialog box opens.
3. Select a printer and click **OK**.

Saving Fabric Manager View Information

Fabric Manager views display information in table format (except Overview View and Topology View). Those tables can be saved and opened in external software applications that reads tab-delimited files.

To save a table:

1. Click any element from the SAN Elements tab.

2. Select **View > View Type**, where *View Type* is any view that displays tables (except Overview View or Topology View).
3. Click **Save Data**. You can also select **Edit > Save Data**. The Save Table to a tab-delimited file dialog box opens.
4. Enter a file name for the table and then click **Save** in the Save Table to a tab-delimited file dialog box. You can open the file in any software that reads tab-delimited files.

Changing At-A-Glance Window Descriptions

When you change an At-A-Glance window description, you change the text that is displayed immediately below the name of the element for which the window is open. You must be in the Overview view to change an At-A-Glance window description.

To change an At-A-Glance window description:

1. Select **View > Overview** to display the Overview view.
2. Click the element from the SAN Elements tab that you want to change the description for.
3. Select **Edit > Change Description**. The Please enter the new description dialog box opens.
4. Enter a description for the pane in the **New Description** field, and click **OK**.
5. Optional: To see the description, click the parent element in the SAN Elements tab. The new description is displayed on the appropriate window.

Logging In to Multiple Devices Simultaneously

You can use Fabric Manager to log in to multiple devices (switches and MP Router) at the same time. With multiple login, you do not need to log in to each device individually to administer your fabric. After you log in to a device, Fabric Manager stores your login information and automatically logs you in to the devices. By default, Fabric Manager stores device passwords to the server. You can disable device passwords from being saved to the server. For more information on disabling device passwords from being saved to the server, see [“Disabling Passwords from Being Saved to the Server”](#) on page 49.

You must log in to a device to perform the all Fabric Manager administrative tasks.

Note: You cannot log in to v4.0 - v4.2 switches with the factory user account in Fabric Manager (although you can from the CLI or Advanced Web Tools). You must use an account with administrative privileges, such as admin, to gain access.

To log in to multiple devices:

1. Select **File > Fabric Login**.
2. Click switches or fabrics from the SAN Elements tab and click the right arrow to move them to the Selected Switches window. You can also drag fabrics or switches to move them to the Selected Switches window.
3. Enter your user ID in the **User ID** field.
4. Enter your password in the **Password** field.

5. Click **Apply**. The success or failure of the login is displayed in the **Status** column of the Selected Switches window. A **Key** icon is displayed next to each switch and fabric that completes a successful login.

The background of the status field changes colors to display its status as follows:

- **Green**: The login was successful. The user ID and password is saved for performing admin operations until the session is terminated. When the session is terminated, this user ID and password is persisted to a file on the Fabric Manager Server. The saved information is used for successive Fabric Manager sessions when Admin operations are initiated from Fabric Manager.
- **Red**: The login failed. The user ID and password are not saved in memory.
- **Yellow**: One of the following:
 - The switch login is being applied; the **Status** column text changes to **Testing**.
 - The switch is **Unreachable** in Fabric Manager. When you add this unreachable switch to the **Selected Switches** list, the **Status** column text changes to **Unreachable**.

Note: If you did not log in to all of the switches successfully, remove the successful switches from the Selected Switches window and retry with a new user ID and password.

Disabling Passwords from Being Saved to the Server

By default, Fabric Manager stores switch passwords to the server. You can disable switch passwords from being saved to the server.

To disable passwords from being saved to the server:

1. Select **File > Options**. The Options dialog box opens (see [Figure 9](#)).

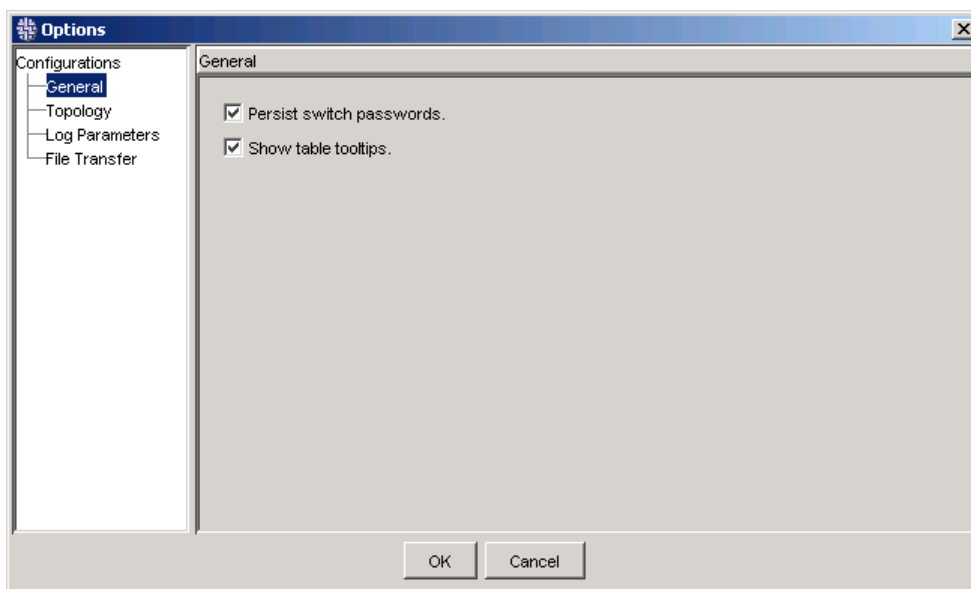


Figure 9: Options Dialog Box

2. To disable switch passwords from being saved to the Fabric Manager server, click **Persist Switch Passwords** (so that the check mark disappears).
3. Click **OK**.

Displaying SAN Elements by IP address, Domain ID, WWN, and Name

Fabric Manager allows you to view SAN elements by the identifier that you find most useful. Because you can identify most SAN elements in multiple ways (for instance, you can identify a switch by IP address, domain ID, WWN, and name), Fabric Manager lets you choose the identifier that you want. When you select identity, you choose the type of identifier that Fabric Manager is displayed for each element.

To select the identifier, click the type of identifier from the ID Menu.

Enabling and Disabling Elements

You can use Fabric Manager to quickly disable or enable large numbers of switches or ports across multiple switches or fabrics. If you disable ports on an MP Router, the port is disabled and stopped. If you enable ports on an MP Router, the port is enabled and started.

To enable or disable elements:

1. Verify that you have logged in to all necessary switches. You cannot enable or disable a port or switch until you log in to that switch. For more information on how to log in, see [“Logging In to Multiple Devices Simultaneously”](#) on page 48. If you are not logged in to the switches, Fabric Manager prompts you to log in before you can proceed.
2. Click the switches, ports, or groups that you want to disable from the SAN Elements tab.
3. Select **Actions > Disable/Enable**, and click the appropriate option.

The results of selecting the switch enable/disable menu item depend on switch status; for example, when the switch is disabled, only the switch enable menu item is enabled and, the switch disable menu item is greyed out, and vice versa. For Telnet, switch enable and disable commands can be executed regardless of switch status.

Setting the Log Level

Note: This feature is for capturing diagnostic information.

Configure log parameters to set the file log severity levels for Fabric Manager log information. When you configure the level of the log, you designate what errors Fabric Managers saves to the file log. Changes made to log levels are dynamic and do not require an application restart to take effect.

To configure log parameters:

1. Select **File > Options**. The Options window is displayed.
2. Click **Log Parameters**.

3. Select **Log Level** > **Level**, where *Level* is one of the following: Debug, Warning, Error, Info, Off, or Fatal. Fabric Manager logs all events of that severity level and lower. Selecting Off disables the logger.
4. Click **OK**.

Downloading a Configuration

You can download a configuration from a baseline file or from a switch. During the download process, you can choose the settings that you want to download and the settings that you want to omit. For instructions on saving a baseline configuration, see “[Saving a Baseline Configuration to a File](#)” on page 90.

Downloading to Switches from a Baseline File

To download a baseline file to one or more switches:

1. Select **Tools** > **Config** > **Compare/Download from File**. The Compare/Download from File -- Select Baseline Configuration dialog box opens.
2. Navigate to the baseline file and click **Open**. The Compare/Download from File -- Target Switch Selection dialog box opens.
3. Click the switches from the SAN Elements tab that you want to compare, and drag them to the right most window. You can:
 - Navigate to a switch, click the switch, and then click the right-pointing arrow.
 - Click and drag a switch from the SAN Elements tab to the right most window.
 - Press and hold Ctrl, click multiple switches in the SAN Elements tab, and click the right-pointing arrow.
 - Press and hold Ctrl, click multiple switches, and click and drag the switches from the SAN Elements tab to the right most window.
 - Click and drag a fabric to the right most window to move or add all of the switches in that fabric to the window.
4. Click **OK**. The Compare/Download from File -- Switch Configuration comparison and Download window opens.
5. Click **Apply Baseline**.

Note: The delay timer at the bottom of the Apply Baseline dialog box cannot be configured from this dialog box. It is propagated from current settings in the sequenced reboot group and represented by the combination of Fabric Stabilization timeout and Delay after Fabric Stabilization parameters.

Prompts display to ensure that you do not accidentally download a configuration.

The Apply Baseline window is displayed. The root navigation tree divides the switches into the following two groups:

- Non-Reboot Config Group: These switches are Linux®-based and do not need to reboot after a config download.
- Reboot Config Group: These switches are VXWorks-based and must reboot after a config download.

6. Click **Apply**. Fabric Manager prompts you to verify that you want to proceed. The download proceeds one group at a time. The status of the switches is displayed in the right window.

Downloading to Switches from a Baseline Switch

To download a configuration from a baseline switch to one or more switches:

1. Select **Tools > Config > Compare/Download from Switch**. The Compare/Download from Switch -- Source Configuration Selection window is displayed.
2. Navigate to the switch that you want to use as a baseline and click the right-pointing arrow to move that switch to the right most window.
3. Click **OK**. The Compare/Download from Switch -- Target Switch Selection window opens.
4. Click switches you want to compare From the SAN Elements tab, and drag them to the right most window. You can:
 - Navigate to a switch, click the switch, and then click the right-pointing arrow.
 - Click and drag a switch from the SAN Elements tab to the right most window.
 - Press and hold **Ctrl**, click multiple switches in the SAN Elements tab, and click the right-pointing arrow.
 - Press and hold **Ctrl**, click multiple switches, and then click and drag the switches from the SAN Elements tab to the right most window.
 - Click and drag a fabric to the right most window to move or add all of the switches in that fabric to the window.
5. Click **Apply Baseline**.

Configuring File Transfer Options

You must set up file transfer options before you can transfer files from a host IP to a remote IP of a switch using File Transfer Protocol (FTP). The FTP server must allow read and write access from the Fabric Manager server for these options to work correctly.

To configure file transfer options:

1. Select **File > Options**. The Options window is displayed (see [Figure 9](#) on page 49).
2. The default view in the Options window is the File Transfer view. If the File Transfer view is not displayed, click **File Transfer** from the Configurations navigation tree. Enter the IP address of your FTP server in the **Remote Host IP** field.
3. Enter your log in name in the **Remote User Name** field.
4. Enter a default FTP directory in the **Remote Directory Path** field. Do not enter a file name; enter only a directory name.
5. Select **Protocol > File Transfer Protocol(ftp)**.
6. Enter your password in the **Password Required for FTP** field.

7. Click **Test** to ensure that you can access the FTP server specified. Fabric Manager reports success or failure. The test must be successful in order for certain features to work (for example, Firmware download, Config download, merge check, and so on).

In addition to validating connectivity to the FTP server, clicking the **Test** button writes a temporary file to the specified FTP directory. In order for the test to complete successfully:

- Write permissions must be set up properly on the specified directory of the FTP server.
- Ports 20 and 21 must be open between the Fabric Manager client, the FTP Server, and the switch.

8. Click **OK** to save settings.

Configuring Notification Parameters

The [Call Home](#) and [Change Management](#) features of Fabric Manager can be configured to send email messages to users when specific changes occur in the defined elements. Before those emails can be sent, you must configure the notification parameters. Notification parameters are global for all users on the Fabric Manager server. Any user can define or modify the notification parameters, and all users on the Fabric Manager server use the same notification parameters.

To configure notification parameters:

1. Select **Tools > Notification Config**. The Notification Config dialog box opens.
If you have already defined the information, either by selecting **Tools > Notification Config** and entering information, or through the Change Management profile configuration, the fields are already populated. You can either leave the information as is, or enter new information.
2. Enter a mail server address, a Change Management from address, and a Call Home from address.
3. Click **Apply**.

Synchronizing Time and Date Across a Fabric

You can synchronize time and date across an entire fabric. You can easily correlate events when you synchronize your fabric, because the firmware timestamps entries in the port log dump.

You must be logged in to switches within a fabric when attempting to set the time on that fabric. The type of fabric configuration determines which switches you must be logged in to. If you are not logged in to the appropriate switches, Fabric Manager prompts you to log in to the appropriate switches before proceeding.

To synchronize time and date:

1. Log in to the switches in the fabric that you want to synchronize. For more information, see [“Logging In to Multiple Devices Simultaneously”](#) on page 48. You can select a fabric, but not a switch group.
2. Click the fabric that you want to synchronize from the SAN Elements tab.
3. Select **Action > Set Time**. The Time dialog box opens (see [Figure 10](#)).

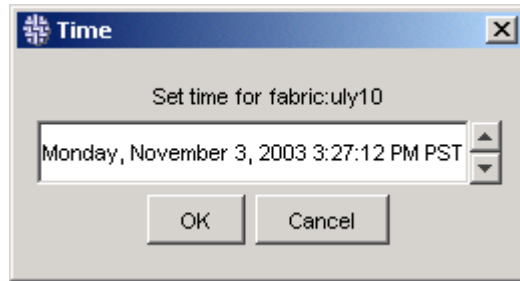


Figure 10: Time Dialog Box

4. To adjust the time or date, click the area in the Time dialog box and use the up and down arrows to change the value.
5. Click **OK**.

Filtering Elements

The Filter tab consists of the following three components:

- A text field
- A pull-down menu
- A SAN Elements field

To filter elements:

1. Click the **Filter** tab.
2. From the pull-down menu, select an identifier. For more information, see “[Filter Tab](#)” on page 26.
3. In the text field, enter text (letters, numbers, or symbols such as a period) that is displayed in the elements that you want to view.

For instance, to view elements that all include *switch* in the name, click **Name** from the pull-down menu and enter *switch* in the text field. To view elements that include 10.32 in the IP address, click **IP** from the pull-down menu and enter 10 . 32 in the text field.

4. Press **Enter**. Every element that includes the text that you entered is displayed in the **SAN Elements** field.

Designating a Switch as a Core Switch

This procedure applies only to Core Edge topologies.

All switches defined in the FCS policy of a secure fabric are considered core switches. Any switches with devices attached to them are automatically considered edge switches. For more information, see [Appendix C](#).

To manually assign a core switch:

1. Click the switch from the SAN Elements tab that you want to designate.
2. Select **Actions > Core Switch**. When you view the fabric to which that switch belongs in Topology View and select the core-edge layout, your switch appears as a core switch.

Monitoring Link Performance

You can monitor link performance in the Topology View.

In relation to links, you can change the threshold percent and the trigger period.

You can change the threshold percent and it immediately takes effect, without having to restart Fabric Manager. If you change the trigger period, you must restart Fabric Manager. The trigger period can be set to a value of 1 to 60 seconds.

The threshold and trigger period are tied to each other. If traffic bandwidth goes over the specified percentage of the actual link bandwidth for the specified period of time, the link in the Topology View turns neon red. If the link is part of a collapsed bundle, the link also turns neon red. The neon red color links go away when traffic bandwidth has gone below the set percentage for the set trigger period.

Setting the Link Threshold Percent

The link threshold percent is for links in the entire fabric, not an individual switch link.

To set the link threshold percent:

1. Select **File > Options**. The Options dialog box opens.
2. Click **Topology**.
3. Enter a value in the threshold percent field.
4. Click **OK** to apply configuration changes.

Setting the Link Trigger Period


To set the link trigger period:

1. Select **File > Options**. The Options dialog box opens.
2. Click **Topology**.
3. Enter a value (in seconds) in the trigger period field. The bandwidth of a link must exceed the threshold percent of the value entered before the link raises a flag. The maximum value allowed is 60 seconds.
4. Click **OK** to apply configuration changes.

Opening a Telnet Session for a Nonsecure Switch

If a Telnet session is already active on a nonsecure switch running firmware versions v2.6.x, 3.0.x, or 3.1.0 and you attempt to launch a new session, a message is displayed asking if you want to close the existing session and launch a new session. If you agree, the active session terminates and a new session is launched.

To open a Telnet session for a nonsecure switch (a switch which does not have secure mode enabled):

1. Click a nonsecure switch from the SAN Elements tab.
2. Select **Actions > Telnet** or click the **Telnet** icon  from the At-A-Glance window of the switch in the Overview view. The Telnet prompt is displayed.
3. Log in as usual.


Displaying the Switch Health Report

Note: The switch health report is available only for switches running firmware versions later than Fabric OS v4.2.x. For switches running 4.2.x or earlier, the switch health report is unavailable and the icon is not displayed in the At-A-Glance view for that switch.

Fabric Manager creates a switch health report that is web based. The report displays the switch state contributors, the status, and the IP address of the switch.

To display the switch health report for a switch:

1. Click a switch from the SAN Elements tab.
2. Select **Actions > Health Report**.

You must be logged in to the switch for the Health Report option to be available. You can also click the **Switch Health Report** icon  from the switch At-A-Glance view, or right-click a switch in the SAN Elements tab, and click **Health Report**.

Fabric Events

4

Viewing Fabric Events with Events View

You can monitor and manage fabric events from the Events view. The Events view allows you to refresh the information on demand, filter events to include only the information you are interested in, save the table, sort the contents, and customize the view.

Refreshing Fabric Events

Fabric events are displayed in the event log table at the switch, fabric, and switch group level. Fabric events are refreshed only on demand. If you want to refresh the information, click **Refresh** in the Events view.

Filtering Fabric Events

You can filter fabric events in the Events view, so that information is displayed only for specific elements.

To filter fabric events:

1. Launch the Events view.
2. Click **Filter**. The Event Filter dialog box opens.
3. Select the filters you want to apply:
 - Optional: Click **by number** and select a number of events. This filter defines how many events are displayed in the Events view at a single time. For a fabric, this is the number of events per switch.
 - Optional: Click **by severity** and select a severity level. This filter displays only events with the specified severity.
 - Optional: Click **by time** to specify a time interval. Click **last** and select a number of hours, or click **between** and select a start and finish time.
4. Click **OK**.

[Table 7](#) describes the fields in the event log table.

Table 7: Event Log Table Fields

Field	Description
Status	Displays the switch status that the event triggered.
Switch	Identifies the switch that experienced the event.
Number	Assigns a number to identify the event in a sequence of events.
Time (host)	Displays the time in the host machine when the event occurred.
Time (switch)	Displays the time on the switch when the event occurred.
Count	Displays the number of consecutive occurrences of the same event.
Level	<p>Displays the severity level of the event. Ascending numbers represent descending severity, as follows:</p> <ul style="list-style-type: none"> ■ 0: panic (switch reboots) ■ 1: critical ■ 2: error ■ 3: warning ■ 4: informational ■ 5: debug
Message	Describes the event.
EventSrc	<p>Indicates the event source, as a daemon or library module. The possible event sources are:</p> <ul style="list-style-type: none"> ■ BLADE ■ BLOOM ■ DIAG ■ EM ■ ERRLOG ■ FABRIC ■ FICON ■ FSSME ■ FW ■ HAM ■ HAMKERNEL ■ MS ■ PD TRACE ■ RCS ■ SULIB ■ SYSC ■ TRACK ■ TS ■ ZONE ■ kSWD ■ syslog

Using the Fabric Watch Module in Fabric Manager

5

For more detailed information regarding the optional Fabric Watch feature, refer to the *HP StorageWorks Fabric Watch 4.2.x User Guide*.

Fabric Watch software monitors the performance and status of switches and can alert you when problems arise. The real-time alerts from Fabric Watch software help you solve problems before they become costly failures. Fabric Manager launches Advanced Web Tools to configure Fabric Watch, so the options that Fabric Manager provides depend on the individual switch and the firmware that runs on the switch. This chapter provides Advanced Web Tools instructions for switches running firmware version 4.2.x. If you have switches running other versions of firmware, refer to the Advanced Web Tools documentation supporting the appropriate version of firmware.

You can configure Fabric Watch software to monitor any of the following:

- Fabric events (such as topology reconfigurations and zone changes)
- Physical switch conditions (such as fan speeds, power supply status, and chassis temperature)
- Port behavior and availability (such as state changes, errors, and performance)
- Small form factor pluggables (SFPs)
- Security events (violations and attempted violations)

Note: The switch must have a Fabric Watch license installed to use this feature.

Some switches are considered a single FRU unit. The Fabric Manager Fabric Watch module does not display FRU class information for those switch types. For more information, refer to the appropriate hardware documentation.

Fabric Watch Terms

Table 8 lists and defines Fabric Watch terms.

Table 8: Fabric Watch Terms and Definitions

Term	Definition
threshold	A configuration of boundaries, traits, and alarms that determine when an event occurs and how Fabric Watch responds to the event.
boundary	A limit (high or low) on the acceptable value of a counter.
counter	The value of the behavior of an element. For instance, the temperature of an SFP or the number of CRC errors.
trait	Behavioral characteristic of a threshold.
alarm	Response to an event.
element	Any component or condition of a switch that Fabric Watch monitors.
event	Behavior of a counter that can trigger an alarm. The following events can trigger an alarm: <ul style="list-style-type: none"> ■ A counter value rises above a high boundary (above event) ■ A counter value falls below a low boundary (below event) ■ A counter value rises above or falls below a range of acceptable values (exceeded event) ■ The value of a counter changes (changed event) ■ A counter value returns from a value outside of an acceptable range to a value within the acceptable range (in-between event)

How Fabric Watch Works

With Fabric Watch software, you can place limits, or *boundaries*, on the behavior of different switch and fabric *elements*. Fabric Watch then monitors these behavior variables, or *counters*, and can issue an alarm when a counter triggers an *event*. An alarm may email you or forward all error information to a proxy switch; the response depends upon how you configure Fabric Watch.

Using Fabric Watch

To use Fabric Watch:

- Select elements that you want to monitor.
- Place limits on the acceptable values of those elements (configure threshold boundaries).

Note: This step applies only when you monitor counters that must remain within boundaries. If you want Fabric Watch to alert you whenever a counter changes, configure an alarm for a changed event.

- Choose if and how Fabric Watch alerts you to errant values (configure threshold alarms).
- Choose whether or not Fabric Watch continues to alert you to persistent errant values (configure threshold traits).
- Enable the thresholds that you configured (configure threshold traits).

Launching the Fabric Watch Module

To access Fabric Watch:

1. Verify that the switch that you want to configure includes a Fabric Watch license.
2. Click the switch you want to configure from the **SAN Elements** tab.
3. Select **Actions > Fabric Watch**.

Advanced Web Tools is launched and you are prompted to log in to the Fabric Watch module. After you successfully log in, the Web Tools **Fabric Watch** module is displayed.

Viewing Alarms

To view alarms:

1. Launch the Fabric Watch module, as described in “[Launching the Fabric Watch Module](#)” on page 61.
2. Click the class that you want to check for alarms in the Fabric Watch navigation tree.
3. Click the **Alarm Notification** tab.
4. Click the area that you want to check for alarms from the **Select Area** menu.

All alarms for that area appear.

For troubleshooting responses to alarms, refer to the *HP StorageWorks Fabric Watch 4.2.x User Guide* for your firmware.

Configuring Threshold Boundaries and Alarms

Configure Fabric Watch boundaries and alarms to designate the circumstances that trigger events and how Fabric Watch responds to those events.

To configure threshold behavior:

1. Launch the Fabric Watch module as described in “[Launching the Fabric Watch Module](#)” on page 61.
2. Click the class that you want to configure to a different behavior in the Fabric Watch navigation tree.

Note: You can set alarms for information on a switch only if that information is monitored by Fabric Watch for that switch; not all alarm options are available for all switches. For more information, refer to the *HP StorageWorks Fabric Watch 4.2.x User Guide*.

3. Click the **Threshold Configuration** tab.
4. Click the area that you want to configure to a different behavior from the **Select Area** menu.

Note: The FRU class is not applicable to switches that are considered a single FRU unit.

5. Click the **Element Configuration** subtab.

6. Click the element that you want to configure to a different behavior from the **Select Element** menu.
7. Click **Triggered** to receive a single alarm once the threshold value has been exceeded. Click **Continuous** to receive continuous alarms once the threshold value has been exceeded. If you click the **Continuous** radio button, enter a time interval in the **Time Interval** menu, or select an interval from the menu.
8. Click **Apply**.

Configuring the Email Server on a Switch

The email notification recipient's DNS server and domain name must be set for each logical switch individually. This means that for each logical switch in a chassis (if applicable), switch 0 and switch 1, you must set up the email notification recipient's DNS server and domain name individually.

To set up the email notification recipient's DNS server and domain name:

1. Select the desired switch from the Fabric Tree. The selected switch is displayed in the Switch view.
2. Click the **Admin** icon from the Switch view. The login screen is displayed.
3. Enter the admin user name and password. The Switch Admin module is displayed.
4. Click the **Switch Information** tab.
5. Enter your primary domain name server IP address in the **DNS Server 1** field in the **Email Configuration** area.
6. Enter your secondary domain name server IP address in the **DNS Server 2** field.
7. Enter the domain name in the **Domain Name** field (between 4 and 32 characters).
8. Click **Apply** to save changes.

Configuring the Email Alert Recipient

A different configuration can be set for each class. For example, one email notification can be set for SFPs and another for E_Ports. Before configuring email alert recipients, you must set up the email notification recipient's DNS server and domain name.

To configure the Email Alert alarm:

1. Launch the Fabric Watch module as described in "[Launching the Fabric Watch Module](#)" on page 61.
2. Click the class that you want configure in the Fabric Watch navigation tree.
3. Click the **Email Configuration** tab.
4. Enter the email address of the administrator who receives email alerts in the **Mail To:** field.
5. Click **Enabled** in the **Mail Status** area.
6. Click **Apply**.

Enabling and Disabling Threshold Alarms

To enable or disable threshold alarms:

1. Launch the Fabric Watch module as described in “[Launching the Fabric Watch Module](#)” on page 61.
2. Click the class with the alarms that you want to enable or disable in the Fabric Watch navigation tree.
3. Click the **Threshold Configuration** tab.
4. Click the area with the alarms that you want to enable or disable from the **Select Area** menu.
5. Click the **Element Configuration** subtab.
6. Click the element in the **Select Element** menu on which you want to enable or disable threshold alarms.
7. Click **Enabled** or **Disabled** in the **Status** area.
8. Click **Apply**. The threshold alarms are enabled or disabled on the element.

Configuring Threshold Behavior

Configure threshold traits to designate if and when Fabric Watch monitors an element.

To configure threshold behavior:

1. Launch the Fabric Watch module as described in “[Launching the Fabric Watch Module](#)” on page 61.
2. Click the class that you want to configure to a different behavior in the Fabric Watch navigation tree.

Note: You can set alarms for information on a switch only if that information is monitored by Fabric Watch for that switch; not all alarm options are available for all switches. For more information, refer to the *HP StorageWorks Fabric Watch 4.2.x User Guide*.

3. Click the **Threshold Configuration** tab.
4. Click the area that you want to configure to a different behavior from the **Select Area** menu.
5. Click the **Element Configuration** subtab.
6. Click the element that you want to configure to a different behavior from the **Select Element** menu.
7. Click **Triggered** to receive a single alarm once the threshold value has been exceeded or click **Continuous** to receive continuous alarms once the threshold value has been exceeded. If you click the **Continuous** radio button, enter a time interval in the **Time Interval** menu, or select an interval from the menu.
8. Click **Apply**.

Displaying a Fabric Watch Alarm Configuration Report

View an alarm configuration report to review information about Fabric Watch settings and thresholds. For detailed information on the configuration report, see [“Configuration Report Tab”](#) on page 67.

To view an alarm configuration report:

1. Launch the Fabric Watch module as described in [“Launching the Fabric Watch Module”](#) on page 61.
2. Click the **Threshold Configuration** tab.
3. Click the **Configuration Report** subtab.
4. Click a previously configured element from the navigation tree.
5. Click the **Alarm** area report to be viewed from the **Area** drop-down menu.
6. Click the **Configuration Report** subtab.

Fabric Watch Dialog Box Reference

The Fabric Watch dialog box provides the fields you need to view and configure for threshold and alarm settings. [Table 9](#) describes the components of the dialog box.

Table 9: Fabric Watch Dialog Box Components

Component	Description
Fabric Watch navigation tree	Displays the various Fabric Watch classes that you can configure. For more information on how to configure Fabric Watch, see “Using Fabric Watch” on page 60.
Alarm Notification tab	Displays Fabric Watch alarms that fabric events have triggered. For more information, see “Alarm Notification Tab” on page 64.
Threshold Configuration tab	Lets you configure threshold boundaries, traits, and alarms. For more information, see “Threshold Configuration Tab” on page 65.
Email Configuration tab	Lets you configure the Fabric Watch Email alert alarm. For more information, see “Email Configuration Tab” on page 67.

Alarm Notification Tab

Use the **Alarm Notification** tab of the Fabric Watch dialog box to view the information for all Fabric Watch elements and classes. The **Alarm Notification** tab polls current events from Fabric Watch and refreshes the display according to the threshold configuration. [Table 10](#) describes the components of the **Alarm Notification** tab.

Table 10: Alarm Notification Tab Component Descriptions

Component	Description
Selected Area pull-down menu	Displays the configurable areas in the pull-down menu. The items listed change, depending on the item selected in the navigation tree.
Name column	Displays the name of the alarm. Threshold names consist of the following three parts, with no separators: <ul style="list-style-type: none"> ■ Class name abbreviation ■ Area name abbreviation ■ Element index number
State column	Displays the severity of the alarm that governs what kind of traps Fabric Watch employs a response to an event. The State of the alarm can be Informative, Normal, or Faulty.
Reason column	Displays the reason that an alarm notification was sent, such as Started, Changed, Exceeded, Below, Above, or In between.
Last Value column	Displays the value of a counter (behavior variable) prior to the alarm.
Current Value column	Displays the value of the counter (behavior variable) that set off the alarms.
Time column	Displays the time and date the notification was sent from the switch.

Threshold Configuration Tab

Use the **Threshold Configuration** tab to view and configure Fabric Watch thresholds for the Fabric Watch class that you select in the Fabric Watch navigation tree. [Table 11](#) describes the components of the **Threshold Configuration** tab.

Table 11: Threshold Configuration Tab Components

Component	Description
Select Area pull-down menu	Lists the areas of thresholds that you can configure. The areas that appear in the pull-down menu depend on the class that you select from the Fabric Watch navigation tree.
Area Configuration tab	Provides fields to configure Fabric Watch threshold boundaries and alarms. For more information, see “Area Configuration Tab” on page 66.
Element Configuration tab	Provides fields to configure Fabric Watch threshold traits. For more information, see “Element Configuration Tab” on page 66.
Configuration Report tab	Displays the Fabric Watch settings for the class that you select from the Fabric Watch navigation tree. For more information, see “Configuration Report Tab” on page 67.

Area Configuration Tab

Table 12 describes the components of the **Area Configuration** tab.

Table 12: Area Configuration Components

Component	Description
Boundary Partition	
Unit field	Set or display the selected unit values used for the chosen area. Depending on the area of interest, this is figured in units of downs, reconfigs, errors, changes, logins, and so on.
High field	Set or display the number of high boundaries (the highest limit at which an element does not trigger an event) for the selected area.
BufferSize field	Set or display the threshold boundary buffer size of the selected area.
TimeBase pull-down menu	Set or display the basic unit of time in which events are recorded for the selected area. The units available from the pull-down menu are: none, second, minute, hour, or day.
Low field	Set or display the number of low boundaries (the lowest limit at which an element does not trigger an event) for the selected area.
Select Boundary Level pull-down menu	Select either a default or custom setting for the boundary levels from the pull-down menu. The default values are shown in parenthesis.
Alarm Setting Partition	
Alarm Notification Mechanisms check boxes.	Select Alarm settings for Errorlog, SNMP, RAN, Portlog and Email to be active on the switch side.
Select Alarm Level pull-down menu	Select either a custom or default setting for the alarm level from the pull-down; this setting is active on the switch side menu.

Element Configuration Tab

Table 13 describes the components of the **Element Configuration** tab.

Table 13: Element Configuration Tab Components

Component	Description
Select Element pull-down menu	Use the pull-down menu to chose a specific element to configure.
Status Partition	
Enable radio button	Select the radio button to enable alarms.
Disable radio button	Select the radio button to disable alarms.
Behavior Type Partition	
Triggered radio button	Select the Triggered Behavior mode if you want Fabric Watch to register an event when a variable exceeds a threshold. An event is not triggered again until the variable falls and exceeds the threshold again.

Table 13: Element Configuration Tab Components (Continued)

Component	Description
Continuous radio button	Select Continuous mode if you want Fabric Watch to register an event when a variable exceeds a threshold and continue to register an event for every time interval.
Time Interval Partition	
Time Interval (in secs) pull-down menu	Select the amount of time (in seconds) that you want Fabric Watch to poll for a new event.

Configuration Report Tab

[Table 14](#) describes the contents of the **Configuration Report** tab.

Table 14: Threshold Configuration Report Component Descriptions

Component	Description
Configuration for Class	Describes the class that is being reported. The item selected in the Navigation tree is displayed here.
Begin Area	Describes the current settings configured for the selected area. see Table 12 .
Begin Element	Describes the current settings configured for the selected area.
Changed	Displays thresholds that have changed.
Exceeded	Displays thresholds that have been exceeded.
Below	Displays thresholds that have fallen below the configured level.
Above	Displays thresholds that have risen above the configured levels.
In between	Displays thresholds that are in within the configured level.

Email Configuration Tab

Use the **Email Configuration** tab to enable and configure email alarm notifications. A different email configuration can be set for each Fabric Watch class. For example, one email notification can be set for SFPs and another can be set for E-Ports (see the navigation tree).

The components of the Fabric Watch Email Configuration are described in [Table 15](#).

Table 15: Email Configuration Component Descriptions

Component	Description
Mail To: field	Accepts the email address that Fabric Watch emails when an event occurs that triggers an email alert.
Mail Status partition	Lets you enable or disable email alert.
Mail Validation partition	Gives you the option to send a test email to the recipient in the Mail To: field when you click Apply .
Apply button	Applies your configuration.
Reset button	Resets the fields to default values.

Change Management

6

The Change Management (CM) feature allows you to monitor changes in a fabric and generate XML reports listing the changes.

To use the CM feature, you must set up profiles defining which elements to monitor, and optionally, when to monitor them, and what to do when changes occur to those elements. The notification configuration defines what to do when changes occur to the selected elements. You do not have to define schedules or notifications. However you must select at least one element to monitor. If you do not define a schedule, there is no automated checking. If you do not define notifications, there can be no alerts or email notifications. You can view the snapshot reports manually, as described in [“Exporting CM Snapshot Reports and Change Reports”](#) on page 76.

The profiles are saved on the server database. Once a profile is defined and saved, any user on the same server can view, edit, or delete it. You can apply a single profile to multiple fabrics, and one fabric can have multiple profiles for different monitoring purposes simultaneously.

If you change the time on a fabric and the end time for a schedule check (as defined in the profile) is subsequently scheduled to before the current time, the report does not run.

If a switch is added to a fabric after a CM profile is created, you must log in to the newly added switch before the profile settings are applied to the switch.

If fabric A is segmented into fabrics A1 and A2, and fabric A has a CM profile associated with it, the fabric that Fabric Manager discovered earlier keeps its CM profile associations. When a fabric segments, CM profile associations are carried forward only to segmented fabrics with the same fabric ID.

If fabric B1 and fabric B2 both have CM profiles associated with them, and you merge the fabrics together, the CM profile for the fabric which was discovered first is applied to the merged fabric.

CM profiles cannot be applied to logical switch groups. To use the CM feature, follow these basic steps:

- Configure notification parameters for all users on the server, as described in [“Configuring Notification Parameters”](#) on page 71.
- Create a Change Management (CM) profile defining which elements to monitor for changes. For more information, see [“Creating a CM Profile”](#) on page 71.
- Optionally, you can compare subsequent snapshot reports to the baseline snapshot report to monitor changes to the elements over time periods.
- Optionally, you can create multiple profiles to monitor different sets of elements. Snapshots are associated with a single profile. However, and a snapshot based on Profile X cannot be compared to a snapshot based on Profile Y.

Change Management Profiles

Set up a Change Management profile that defines which elements you want Fabric Manager to monitor. You can also define when to monitor them, and what to do when changes occur to the selected elements (email notification and/or alerts). For added clarification in this document, the Change Management profiles are called CM profiles.

You can manage the following types of changes using the CM profiles:

- ISL changes
- Switches added to or removed from the fabric
- Switch configuration changes
- Zoning changes
- Name server changes
- Firmware version changes
- Licenses added or removed from switches in the fabric
- Port status: Only not-configured/disabled, offline, and online statuses are reported. Down status is not reported.
- Device links: The change report, if defined in the profile, identifies the domain and port WWN the device connects to.
- Security mode enabled or disabled
- Security policy changes

The MP Router behaves differently with the Change Management feature, as follows:

- If a fabric includes an MP Router as a member switch (not the launch switch), switch configuration changes are not reported for the MP Router. In addition, Fabric Manager might not be able to collect security policy change information for the entire fabric if the MP Router is the first object Fabric Manager gets from API.
- If a fabric includes an MP Router as a launch switch, the following Change Management information cannot be retrieved for that switch (because the MP Router does not support these elements):
 - ISL changes
 - Zoning changes
 - Switch configuration changes
 - Security mode enabled or disabled
 - Security policy changes

Snapshot Reports

Once you define a profile, a snapshot report displays the information for the elements defined in the profile. The first snapshot report created for a profile is automatically saved as the *baseline* snapshot report. All subsequent snapshot reports are compared to the baseline snapshot report. Each profile can have multiple associated snapshots. In the profiles, you can edit the time intervals and specifications for monitoring, and what to do when the changes occur, but you cannot change which elements to monitor. To monitor a different set of elements, you must create a new profile.

Because snapshot reports are stored on the Fabric Manager server, depending on the number of checks you are running and the size of your fabric, you might require large volumes of disk space.

Configuring Notification Parameters

You can configure notification parameters for Change Management email notifications and the Call Home email notifications on a global basis; all users on a server share the same configuration values. The configuration information is stored in the Fabric Manager database and persists across client and server reboots.

You must specify an email address of the site mail server host for both, Change Management and Call Home features.

Once you have configured the notification parameters, you can specify for the server to do the following in the CM profile:

- Send you an email with snapshot and change reports attached in XML format
 - When there is no change during the scheduled checking.
 - When there are changes during the scheduled checking.
- Create alerts in the Alerts View if changes occur during the scheduled checking. Once an alert is displayed in the Alerts View, the time and description on the alert is updated every time there is another change; subsequent alerts are not generated for subsequent scheduled checks. If subsequent changes do not occur, the alert status is automatically set to resolved.

You must configure notification parameters before specifying that you get email notifications or reports for Change Management or Call Home.

To configure notification parameters:

1. Select **Tools > Notification Config**. The Notification Config dialog box opens.
2. Enter the Mail Server email address.
3. Enter the Change Management from address. This is the address that is used to send the CM reports from.
4. Enter the Call Home from address. This is the address that is used to send the Call Home reports from.
5. Click **Apply**.

Creating a CM Profile

To create a CM profile:

1. Select **Tools > ChangeMgmt > Manage Profiles**. The Change Management Profiles dialog box opens. Any existing profiles are displayed in the dialog box.
2. Click **New Profile**. The Change Management wizard is displayed.
3. Read the introduction and then click **Next**.
4. Enter a profile name and click the check boxes next to the parameters you want to monitor for changes, as displayed in [Figure 11](#).

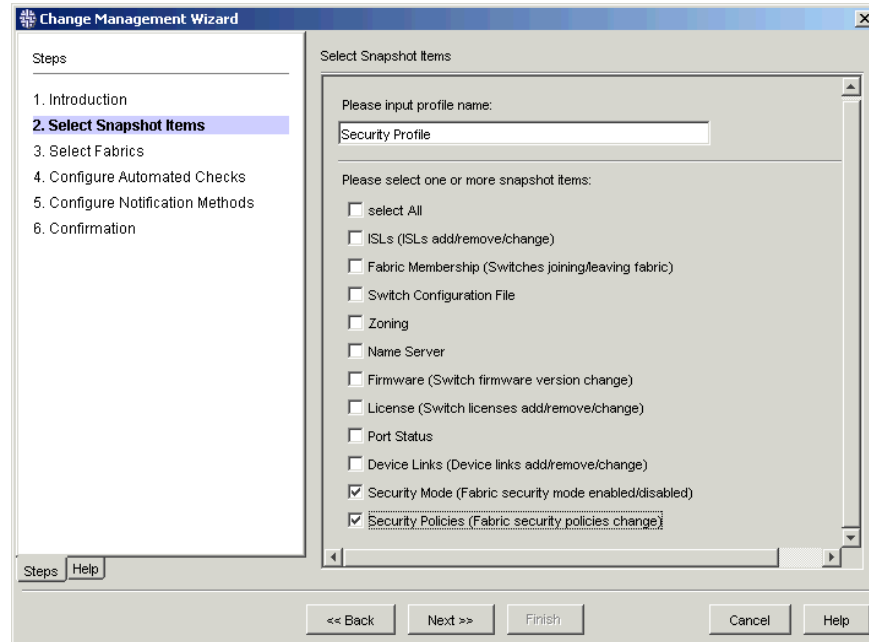


Figure 11: Change Management Snapshot Items

5. Click **Next**.
6. Click the fabric or fabrics from the **SAN Elements** tab in the Change Management wizard that you would like to include in the profile. Click the right arrow button to add them to your selection.
7. Click **Next**. All switches in selected fabrics must be logged in. A switch log in dialog box opens if the log in information is not set yet. Enter the switch login information.
8. If you do not want to set up an automated schedule to perform the checks, click **Configure schedule later** and then click **Next**.

If you want to set up a schedule for the checking:

- a. Click **Take Snapshots per this schedule**.
- b. Click an element in the **Start Time** field and use the scroll buttons to change the day and time to show when you want to begin checking the selected fabrics for selected parameter changes.
- c. Click an element in the **End Time** field and use the scroll buttons to change the day and time to show when you want to stop checking the selected fabrics for selected parameter changes. If you do not want to stop the checking, click the **no end date** radio button.
- d. Enter a number in the **frequency** field and select hours, days, or weeks from the pull-down menu. If you want to run the check only once, select **once** from the frequency pull-down menu.
- e. Enter a number of days to keep the check reports. The minimum is 1 and the maximum is 2147483647.
- f. Click **Next**.

9. If you would not like to receive email notifications or alerts when changes occur, click **Next** to skip this step. If you would like to receive notifications when changes occur:
 - a. Optional: Click **Send email notification when changes occur** to receive email notifications. You receive an xml attachment in an email listing exact changes based on the parameters you specified in the profile.
 - b. If you selected to receive email notifications in step a, you must enter at least one email address. Optional: You can send a test email to the addresses specified by clicking **Test**.
 - c. Optional: If you want to get an email notification even when there is no change, click **Send email even if there is no change**.
 - d. Optional: Click **Send alert when changes occur** if you want alerts to be triggered for CM changes defined in this profile. Select an alert level for the CM alerts.
 - e. Click **Next**.

A confirmation page is displayed with the settings you have selected for the CM profile.

10. Verify the settings and then click **Finish**.

Fabric Manager saves the CM profile information to the database. The first snapshot report created is saved as the baseline snapshot report. All subsequent snapshots are compared against the baseline snapshot, and the comparison report (change report) is displayed in the subsequent snapshots.

All snapshots are saved in the database. They are purged when you specified to purge them, or they can be manually deleted. If a switch or fabric is removed from Fabric Manager, all associated profiles and snapshots are deleted.

Now that you have created a CM profile, you can edit, delete, and clone the profile. You can also create additional profiles.

You can view, print, delete, and export the snapshot reports created.

Displaying Saved CM Profiles

You can display all saved change management profiles on the server, and you can display which fabrics are using the profiles.

To display saved CM profiles:

Select **Tools > ChangeMgmt > Manage Profiles**. The Change Management Profiles dialog box opens. Any existing profiles are displayed in the dialog box.

Deleting CM Profiles

When you delete a CM profile, all associated snapshots and change reports are also deleted from the database.

To delete CM profiles:

1. Select **Tools > ChangeMgmt > Manage Profiles**.

The Change Management Profiles dialog box opens. Any existing profiles are displayed in the dialog box.

2. Click one or more CM profile from the table, and click **Delete Profile**. A confirmation dialog box opens.
3. Click **OK** to delete the selected profiles, and all snapshots and change reports based on the selected profiles, from the database.

Editing CM Profiles

To edit a CM Profile:

1. Select **Tools > ChangeMgmt > Manage Profiles**. The Change Management Profiles dialog box opens. Any existing profiles are displayed in the dialog box.
2. Click the profile you want to edit, and click **Edit Profile**. The Change Management wizard is displayed.
3. Read the introduction and then click **Next**.
4. The name of the profile you selected in [step 2](#) is in the Please Input Profile Name dialog box. If you want to edit another profile, enter the profile name now.
5. Click **Next**.
6. Optional: Rearrange the fabrics you want to monitor for changes by clicking them to select the fabric, then using the right and left arrow keys to move them back and forth.
7. Click **Next**.
8. Optional: Configure automated checks. Click **Next**.
9. Optional: Configure Notification Methods. Click **Next**.
10. Read the confirmation and click **Finish**.

Duplicating (Cloning) Existing CM Profiles

You can clone (duplicate) CM profiles. This is useful in the case where you have another fabric that you want to run the same or very similar checks on. You do not need to go through the entire process of creating a new profile. You can duplicate an existing profile and make any changes you wish.

To clone a CM profile:

1. Select **Tools > ChangeMgmt > Manage Profiles**. The Change Management Profiles dialog box opens. Any existing profiles are displayed in the dialog box.
2. Click one CM profile from the table, and click **Clone Profile**. The Clone Profile wizard is displayed.
3. Read the introduction and click **Next**. The information from the selected profile is copied to the new profile and is displayed in the wizard.
4. Optional: Change the profile name and elements to monitor.
5. Optional: Select a new fabric for the new profile.
6. Click **Next**.
7. Optional: Make changes to the schedule.
8. Click **Next**.
9. Optional: Make changes to the notification settings.

10. Click **Next**. A confirmation is displayed indicating the selected settings for the cloned CM profile.
11. Verify the settings and then click **Finish**.

Fabric Manager saves the CM profile information to the database. Fabric Manager creates snapshots based on the specifications in the CM profile and saves those snapshots to the database. The snapshot for each fabric is saved as a baseline.

If you have scheduled automatic checks, the Fabric Manager server also creates scheduled tasks to automatically create snapshots and generate change reports against the baseline. All reports and snapshots are saved in the database.

You can save, export, and print the report you created. You can also create additional profiles and compare them.

Displaying a Change Report

All subsequent snapshots are compared to the baseline snapshot report, and change reports are automatically created that list the changes between the baseline snapshot and the subsequent snapshot.

To manually compare a live CM snapshot to a baseline configuration:

1. Select **Tools > ChangeMgmt > View Change Reports**. The Fabric Picker dialog box opens.
2. Select a fabric to view change reports for, click the right arrow icon to move it to the right window and click **OK**. The Change Management Reports dialog box for that switch displays a list of profiles and associated snapshots for that fabric.
3. Click a snapshot report (other than the baseline) to view the change reports.
4. Click **View** under the **Change Reports** area. The Change Report is displayed (see [Figure 12](#)).

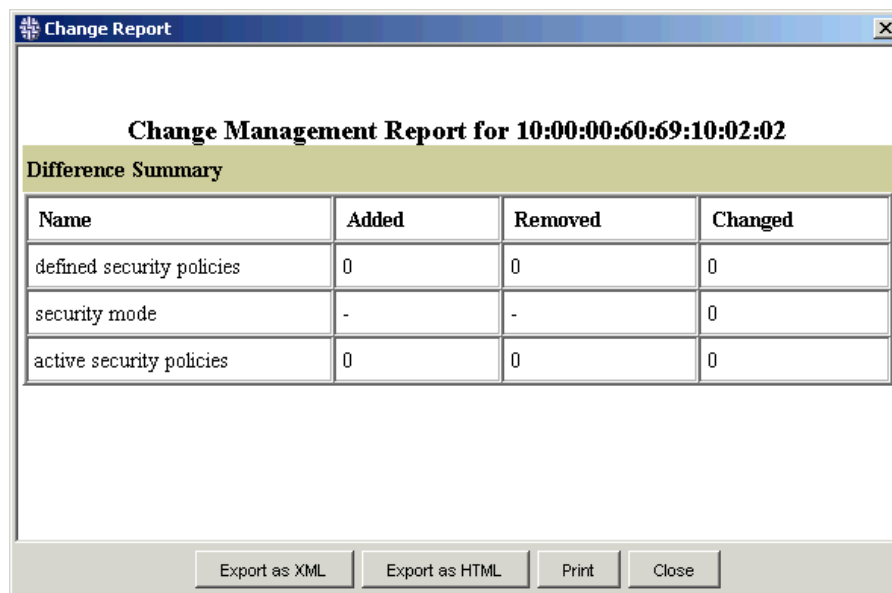


Figure 12: Change Management Change Report

You can export the report as XML, export the report as HTML, or print the report.

Creating CM Snapshots on Demand

To create a snapshot on demand:

1. Select **Tools > ChangeMgmt > View Change Reports**. The Fabric Picker dialog box opens.
2. Select a fabric to view change reports, click the right arrow icon to move it to the right window, and then click **OK**. The Change Management Reports dialog box for that switch displays a list of profiles and associated snapshots for that fabric.
3. Click a snapshot from the list and then click **Take Now**. The Change Report is displayed.

Comparing Two CM Snapshots to Each Other

To compare two snapshots to each other:

1. Select **Tools > ChangeMgmt > View Change Reports**.
2. Click one fabric to view its change reports and then click **OK**. The Change Management Reports dialog box opens, listing all of the existing profiles, associated snapshots, and change reports for that fabric.
3. Click two snapshots from the table (associated with the same CM profile) and then click **View Change Report**.

Exporting CM Snapshot Reports and Change Reports

To export CM reports:

1. Select **Tools > ChangeMgmt > View Change Reports**. The Fabric Picker dialog box opens.
2. Select a fabric to view its change reports, click the right arrow icon to move it to the right window, and then click **OK**. The Change Management Reports dialog box for that switch displays a list of profiles and associated snapshots for that fabric.
3. Click a snapshot report or change report.
4. Click **View**.
5. Click **Export as HTML** to export the Change Report as an HTML file. Click **Export as XML** to export the Change Report as an XML file. The Save dialog box opens.
6. In the Save dialog box, enter a name for the file, browse to the location where you want to save the file, and then click **Save**.

Displaying CM Change Reports (XML Format) in External Applications

When you select to export CM change reports in XML format, an `xslt` file (stylesheet) is also saved with the XML file. The `xslt` file can be used to translate the XML file into an Excel spreadsheet (or other software applications that allow you to open XML file types). You can then edit the information in the spreadsheet.

You do not need to use the `xslt` file provided by Fabric Manager, or any `xslt` file; however, if you do not use a stylesheet, the translated information is not very useful.

The following procedure uses Excel 2000 as a sample application in which you can open the XML file to manipulate the performance monitor data. There are other applications you can open XML files in as well.

To open a CM change report saved in XML format in Excel:

1. Launch Excel 2002 (or later).
2. Select **File > Open**. The Open dialog box opens.
3. Navigate to the XML file, and click **Open**. The Import XML dialog box opens, asking you if you would like to open a stylesheet.
4. Click **Open the file without applying a stylesheet** (not recommended) or click **Open the file with the following stylesheet applied**.

If you clicked **Open the file without applying a stylesheet**, the information is displayed in an Excel spreadsheet without the formatting.

If you clicked **Open the file with the following stylesheet applied**, the `xslt` file created by Fabric Manager is the default selected file. You can either use that file, or navigate to another stylesheet of your own.

5. Click **OK** to display the information in an Excel spreadsheet.

Printing CM Snapshot and Change Reports

To export CM reports:

1. Select **Tools > ChangeMgmt > View Change Reports**. The Fabric Picker dialog box opens.
2. Select a fabric to view its change reports, click the right arrow icon to move it to the right window, and then click **OK**. The Change Management Reports dialog box for that switch displays a list of profiles and associated snapshots for that fabric.
3. Click a snapshot report or change report.
4. Click **View**.
5. Click **Print** to print the change report.

Changing Baseline Snapshot Reports

To change a baseline snapshot report:

1. Select **Tools > ChangeMgmt > View Change Reports**. The Fabric Picker dialog box opens.
2. Select a fabric to view its change reports, click the right arrow icon to move it to the right window, and then click **OK**. The Change Management Reports dialog box for that switch displays a list of profiles and associated snapshots for that fabric.
3. Click a snapshot report (other than the baseline) that you want to select as the new baseline snapshot report.
4. Click **Change Baseline**. A confirmation is displayed, indicating that all previous change reports (compared to the previous baseline) are to be deleted.
5. Click **Yes** in the confirmation window to proceed. A dialog box opens, asking if you want to regenerate all change reports based on the new baseline.

6. Click **Yes** to generate new change reports. A confirmation is displayed, indicating that the baseline has been change successfully. Click **OK**.

Click **No** if you do not want to generate new change reports. A confirmation is displayed, indicating that the baseline has been change successfully. Click **OK**.

Click **Cancel** if you do not want to change the baseline switch anymore. The baseline is not changed, and you are brought back to the Change Management Reports dialog box.

Name Server

7

Fabric Manager launches Advanced Web Tools to display name server entries listed in the Simple Name Server database. This includes all Name Server entries for the fabric, not only those related to the local domain. Each row in the table represents a different device. This chapter provides Advanced Web Tools instructions for switches running firmware version 4.2.x. If you have switches running other versions of firmware, refer to the Advanced Web Tools documentation supporting the appropriate version of firmware.

Note: The polling interval for the Name Server information is every 30 seconds.

Table 16 describes the items in the Name Server Table.

Table 16: Name Server Table Entries

Field or Button	Description
Auto Refresh	Check to enable Auto Refresh. Un-check to disable Auto Refresh.
Auto Refresh Interval	Enter the number of seconds for the refresh interval if Auto Refresh is checked.
Refresh	Select to refresh the window immediately.
OK	Select to close the window.
Domain #	The domain ID of the switch to which the device is connected.
Port #	The number of the switch port to which the device is connected.
Port Name	Displays the name of the port. This option is available only on switches running firmware versions 3.1.0 or 4.1.0.
Port ID	The port ID of the device (24-bit hexadecimal value).
Port Type	The port type of the device, where: N = fabric direct attached port NL = fabric direct attached loop port
Fabric Port WWN	The worldwide name of the fabric port.
Device Port WWN	The worldwide name of the device port.
Device Node WWN	Displays the worldwide name of the device node.
Device Name	Displays the symbolic name of the device assigned through the <code>SCSI inquiry</code> command.
FC4 Types	Displays the Fibre Channel FC4 layer types supported by the device, such as IP or FCP.
COS	Displays the Fibre Channel classes of service supported by the device.
Port IP Address	Displays the IP address of the fabric port.
Hard Address	Displays the hard address of the fabric port.
Member of Zones	Displays the zones to which this device belongs. This column does not update when the table is refreshed. To view updated zoning information, close and re-open the Name Server Table.

Displaying Name Server Entries

Advanced Web Tools displays Name Server entries listed in the Simple Name Server database. This includes all Name Server entries for the fabric, not only those related to the local domain. Each row in the table represents a different device.

Note: Name Server entries are not automatically polled by default. You must click **Refresh** from the Name Server window to poll Name Server entries.

You can also specify a time interval at which the Name Server entries are to be refreshed. Click the **auto-refresh** box and enter a time value (in seconds) in the **auto-refresh interval** field. Click the **auto-refresh** box again to save the changes.

To display Name Server entries:

1. From the SAN Elements tab, click the fabric for which you want to see the Name Server entries.
2. Select **Actions > Name Server**. Advanced Web Tools launches and displays the Name Server information.
3. Optional: Check the **Auto Refresh** check box from the Name Server window.
4. Enter an auto refresh interval, at a minimum of 15 seconds. The Name Server entries are refreshed at the rate you set.

Displaying Name Server Information for a Device

To display Name Server information for a particular device:

1. Launch the Name Server Entries table, as described in “[Displaying Name Server Entries](#)” on page 81.
2. Click a device from the **Domain** column and then click **Detail View** in the Name Server information window. The Name Server Information dialog box displays information specific to that device.

Displaying Zone Members of a Device

To display the Zone Members of a particular device:

1. Launch the Name Server Entries table, as described in “[Displaying Name Server Entries](#)” on page 81.
2. Click a device from the **Domain** column and then click **Accessible Devices**. The Zone Accessible Devices dialog box displays accessible zone member information specific to that device.

Fabric Topology

8

You can choose from among the fabric topology layouts that Fabric Manager is displayed in the Topology view. You can select from the following layouts:

- **Circular Layout:** Lays out the ring/star topologies in a way that preserves the visual identity of each cluster and avoids overlapping nodes and clusters.
- **Core-Edge Layout:** The core-edge layout is the default layout. Visually separates core switches, edge switches, and nodes. By default, when a nonsecure fabric is discovered, all switches with devices attached are marked as edge switches. All switches without devices attached are marked as core switches.

All switches defined in the FCS policy of a secure fabric are considered core switches. Any switches with devices attached to them are automatically considered edge switches. You can assign a core switch manually. For instructions, see “[Designating a Switch as a Core Switch](#)” on page 54.








- **Tree Layout:** Organizes the fabric hierarchically.

Fabric Manager supports logical SANs, and the Topology view displays the virtual switches and links in the SANs.

Links

The lines that connect icons in Topology view represent different varieties of links in the fabrics. [Table 17](#) displays the link images and explains the meaning of each.

Table 17: Topology View Link Images

Image		Description
	Bundled links	Represents all links between two switches to reduce clutter in the topology display. Double-click the bundle to expand it.
	Expanded bundle	Displays the individual links that form a bundle. Double-click the expanded bundle to collapse the links into a bundle.
	1 Gbps link	Represents a 1 Gbps link between two switches. When you enable ISL Checking, this link appears as red, yellow, or green based on the ISL Checking status of the link.
	2 Gbps link	Represents a 2 Gbps link between two switches. When you enable ISL Checking, this link appears as red, yellow, or green based on the ISL Checking status of the link.
	Trunked links	Represents a trunk between two switches. This link appears as red, yellow, or green based on the ISL Checking status of the link.
	Device groups	Represents the devices that connect to a switch. Double-click the device group to open a window that displays the devices in table format.
	Device links	Represents the link between a switch and the devices that connect to it.

Viewing Your Fabric with Topology View

Topology view provides a graphical representation of your fabric. For detailed information on Topology view, see [Appendix C](#).

Note: Topology view might take a considerable amount of time to open. Topology view options might also respond slowly.

After you click a fabric in the **SAN Elements** tab, you can perform the following tasks to view more information about your fabric:

- Click and hold on any element in the view to display a tooltip. Tooltips provide basic information about the element that you clicked. Tooltips disappear when you release the mouse button.
- Double-click a device group to open a window that displays each device in the group in detail. This window also provides a Print option.
- Double-click a bundled link to view the individual links that compose the bundle. Double-click the individual links to view the bundle again. When you double-click a bundle, you can then view tooltips on each individual link. The tooltip includes the bandwidth, and the ports and switches to which the ISL connects.

You cannot expand a bundle when you engage the **Select** icon.

- Click the **Select** icon in the toolbar to move nodes in the display. Fabric Manager stores the changes that you make to the locations of the nodes.
- Graphically view ISL Checking events and Fabric Checking events.
- Click the **SnapShot** icon to save an image file of your topology. You can use this file as a baseline and compare your fabric to it at a later time.
- From the **Layout** menu, select **Circular**, **Core-Edge**, or **Tree** to view your fabrics from different perspectives.

Assigning a Core Switch Manually

Note: You can assign a core switch only in the Core Edge topology layout.

To assign a core switch manually:

1. Click a switch from the **SAN Elements** tab.
2. Select **Actions** > **Core Switch**. A check mark is displayed next to **Core Switch** in the **Actions** menu, indicating that the switch is selected as the core switch.

Configuring Topology View Options

To configure Topology view options:

1. Select **File > Options**. The Options dialog box opens.
2. Click **Topology**.
3. Select a layout from the **Default Startup Layout** menu. The available options are **Circular**, **Core Edge**, and **Tree**.
4. Select a link style from the **Default Startup Link Style** menu. The available options are **Orthogonal** and **Straight**.
5. Select a default link bundle state from the **Default Link Bundle State** menu. The available options are **Expanded** and **Collapsed**.

Note: The existing bundled links do not change to reflect your selection; however, newly added bundled links do reflect your selection.

6. Select a tile direction from the **Tile Direction** menu. The available options are **Vertical** and **Horizontal**.
7. Enter a threshold percent in the **Threshold Percent** field.
8. Enter a threshold trigger period in the **Threshold Trigger Period** field.
9. Click **OK**.

Viewing Discovered Fabric Topologies

To view discovered fabric topologies:

1. Select **View > Topology**.
2. Click a SAN or fabric from the **SAN Elements** tab. The **SAN** or **Fabric** node is displayed in the **View** area.

Note: To view a specific section of a large fabric in a different window, select the **Overview** icon from the **Topology** menu.

3. Click the **+** to expand the view to the desired level. The **Fabric** node disappears and an outlined sub-graph is displayed.
4. Click the **-** to collapse the sub-graph back to the Fabric view.

Taking a Snapshot of a Topology

To take a snapshot of a topology:

1. Select **View > Topology**.
2. Click a SAN or fabric from the **SAN Elements** tab. The **SAN** or **Fabric** node is displayed in the **View** area.
3. Click the **Snapshot** icon from the Topology toolbar. The Snapshot window is displayed.
4. Click the **Export to PNG** icon. The Export as PNG file window is displayed.
5. Save a PNG version of the topology snapshot to a folder.

Note: The snapshot captures only what you see in the current Topology window, and does not capture anything that is not visible on the screen.

Moving a Topology Object

To move a topology object:

1. Select **View > Topology**.
2. Click a SAN or fabric from the **SAN Elements** tab. The **SAN** or **Fabric** node is displayed in the **View** area.
3. Click the arrow icon from the Topology toolbar.

Note: Tooltips are disabled while using the select arrow, pan, or interactive zoom features.

4. Click and drag a node using the mouse.

Comparing Configurations

9

Fabric Manager can compare the configuration files of your switches to a *baseline* configuration to:

- Validate and ensure consistent configuration settings among the switches in your fabric.
- Propagate configuration settings to switches in your fabric.
- Store a selection of configuration settings that you can easily propagate throughout your fabric.
- Troubleshoot a switch.

[Table 18](#) explains the two sources that Fabric Manager can use as baselines.

Table 18: Baseline Sources

Source	Explanation
Switch	Compare multiple switches to one switch that you identify as a baseline.
File	Save the configuration file of a switch as a file on a FTP server and then compare switches to that file or propagate that file to switches.

You can save portions of a configuration to a file so you can propagate fabric-wide settings but leave switch-specific settings untouched. For instance, you can save Fabric Watch configuration settings to a baseline and then propagate those settings to an entire fabric and not alter the switch name of any switch in the fabric.

You can also use Change Management to back up configuration files automatically.

Best Practices

The following best practices describe tasks you can perform with the Save Baseline tool to administer your fabric more efficiently.

- Propagate a baseline configuration to each new switch that you add to a fabric to ensure that the switch is compatible with the fabric.
- Propagate the baseline of one fabric throughout a second fabric before you merge the fabrics.
- Propagate a baseline configuration throughout a fabric to ensure consistent Fabric Watch and Simple Network Management Protocol (SNMP) settings.
- Create and store multiple baselines that serve different purposes so you can quickly adapt your fabric when it switches function.
- Create a limitless number of baselines.
- Use baselines to recover fabric and switch settings.

Saving a Baseline Configuration to a File

Note: If you just discovered a fabric and want to save a baseline, wait about 60 seconds to let Fabric Manager discover all port, device, and ISL information. If you do not wait, you receive incomplete results when you run the baseline compare.

Save a baseline from a single switch in a fabric. You can export the following categories of information from the configuration file to the baseline:

- Settings that you can normally assign with the `configure` command
- Settings for Fabric Watch and SNMP

When you create your baseline, Fabric Manager gives you the opportunity to choose what settings you want to add to the baseline and what settings you want to omit from the baseline.

Before saving a baseline configuration to a file, you must set up configuration file transfer properties between switches and your host.

To save a baseline:

1. Configure file transfer settings if you have not already done so. For more information, see [“Configuring File Transfer Options”](#) on page 52.
2. Log in to the switch with the configuration that you want to save as a baseline. For more information, see [“Logging In to Multiple Devices Simultaneously”](#) on page 48.
3. From the **Tools** menu, select **Config > Save Baseline**. The Save Baseline -- Configuration Template Selection dialog box opens.
4. Select **Full Configuration** and click **Next**. The Save Baseline -- Switch Selection window opens.
5. From the **SAN Elements** tab, choose the switch with the configuration that you want to save and then click the right-pointing arrow to add it to the right most window.
6. Click **OK**. The Save Baseline -- Parameter Selection window opens.

7. Check the check boxes for each setting or group of settings of the configuration file that you want to save to the baseline. Expand and collapse the navigation tree to access your options.

Note: The Solaris environment does not display check boxes clearly. If the check box is full, the value is selected. If the check box is shallow, it is not selected.

8. Click **Save**. The Save base file dialog box opens.
9. Enter a name for your baseline, choose a folder to store it, and click **Save**.

Comparing Switches to a Baseline

When you compare the configuration of a switch to a baseline, Fabric Manager identifies and lists all parameters that do not match. Compare the configuration of one or more switches to a baseline when:

- You plan to merge two fabrics.
- You plan to add a new switch to a fabric.
- You want to verify that Fabric Watch and SNMP settings are consistent across a fabric.
- A fabric segments and you need to troubleshoot the problem.

Note: If you just discovered a fabric and want to run Fabric Backup or Diff with Backup, wait about 60 seconds to let Fabric Manager discover all port, device, and ISL information. If you do not wait, you receive incomplete results when running the Fabric Backup or Diff with Backup.

Comparing Switches to a Baseline File

To compare switches to a baseline file:

1. From the **Tools** menu, select **Config > Compare/Download from File**. The Compare/Download from File -- Select Baseline Configuration dialog box opens.
2. Navigate to the baseline file and click **Open**. The Compare/Download from File -- Target Switch Selection window opens.

Note: In a Solaris environment, make sure you select a directory, not the actual file, to compare the configuration against.

3. From the **SAN Elements** tab, select the switches that you want to compare and move them to the right most window. You can:
 - Navigate to a switch, click the switch, and then click the right-pointing arrow.
 - Click and drag a switch from the **SAN Elements** tab to the right most window.
 - Press and hold **Ctrl**, click multiple switches in the **SAN Elements** tab, and click the right-pointing arrow.

- Press and hold **Ctrl**, click multiple switches, and click and drag the switches from the **SAN Elements** tab to the right most window.
 - Click and drag a fabric to the right most window to move or add all of the switches in that fabric to the window.
4. Click **OK**. The Compare/Download from File -- Switch Configuration comparison and Download window is displayed and compares the configurations of the switches to the baseline.
 5. To apply this baseline to the switches that you selected, click **Apply Baseline**.

Comparing Switches to a Baseline Switch

To compare switches to a baseline switch:

1. From the **Tools** menu, select **Config > Compare/Download from Switch**. The Compare/Download from Switch -- Source Configuration Selection window opens.
2. Navigate to the switch that you want to use as a baseline and click the right-pointing arrow to move that switch to the right most window.
3. Click **OK**. The Compare/Download from Switch -- Target Switch Selection window opens.
4. From the **SAN Elements** tab, select switches you want to compare and move them to the right most window. You can:
 - Navigate to a switch, click the switch, and then click the right-pointing arrow.
 - Click and drag a switch from the **SAN Elements** tab to the right most window.
 - Press and hold **Ctrl**, click multiple switches in the **SAN Elements** tab, and click the right-pointing arrow.
 - Press and hold **Ctrl**, click multiple switches, and click and drag the switches from the **SAN Elements** tab to the right most window.
 - Click and drag a fabric to the right most window to move or add all of the switches in that fabric to the window.
5. Click **OK**. The Compare/Download from Switch -- Switch Configuration comparison and Download window is displayed and compares the configurations of the switches to the baseline.
6. To apply this baseline to the switches that you selected, click **Apply Baseline**.

Customizing Baseline Templates

When you save a baseline configuration, Fabric Manager requires that you choose a configuration template. The templates display in the Save Baseline -- Configuration Template Selection (Figure 13).

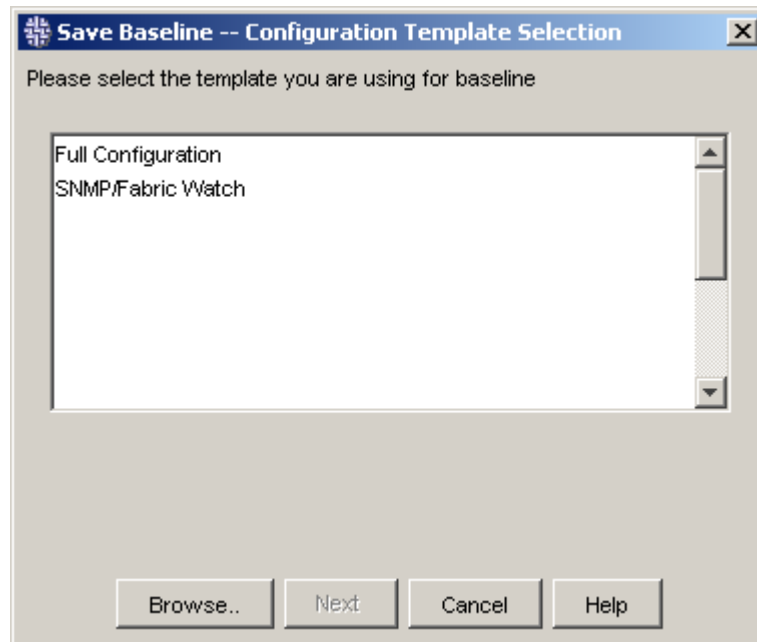


Figure 13: Template Selection

The template that you choose determines what parameters appear in the Save Baseline -- Parameter Selection dialog box (Figure 14).

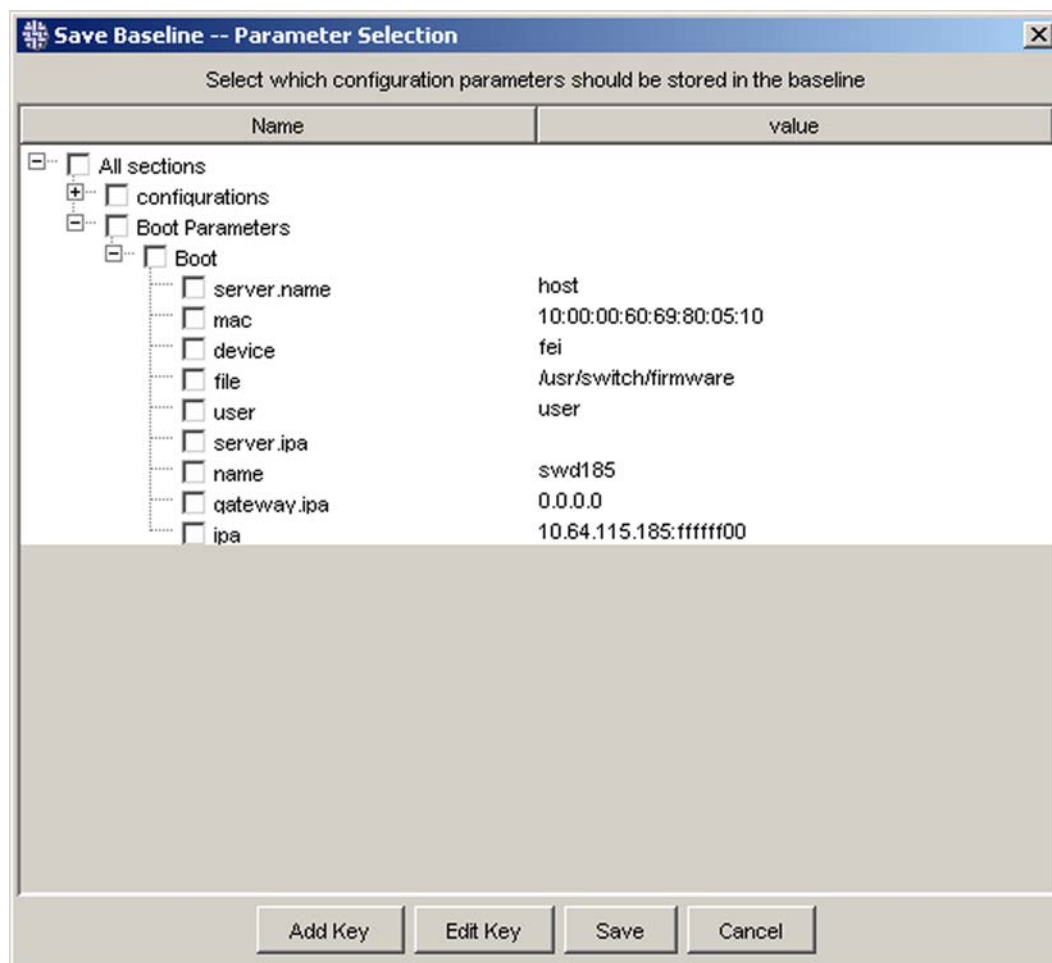


Figure 14: Parameter Selection

Fabric Manager provides two templates, but you can create custom templates or edit the existing templates. To create a custom template, create an XML file (as defined below) and save it in the Fabric Manager > baseline > template directory on your Fabric Manager server. The **Full Configuration** and **SNMP/Fabric Watch** template files appear in this directory.

Anatomy of Template Files

To customize a baseline template file, you must define custom XML tags. This section describes those tags.

Description Tag

The **Description** tag encloses the summary tag, which defines what template title is displayed in the Save Baseline -- Configuration Template Selection dialog box. The example that follows displays My Template in the dialog box.

Example

```
<Description>
  <summary>My Template</summary>
  <detail>This will show my custom parameters</detail>
</Description>
```

The results of this configuration are shown in [Figure 15](#).

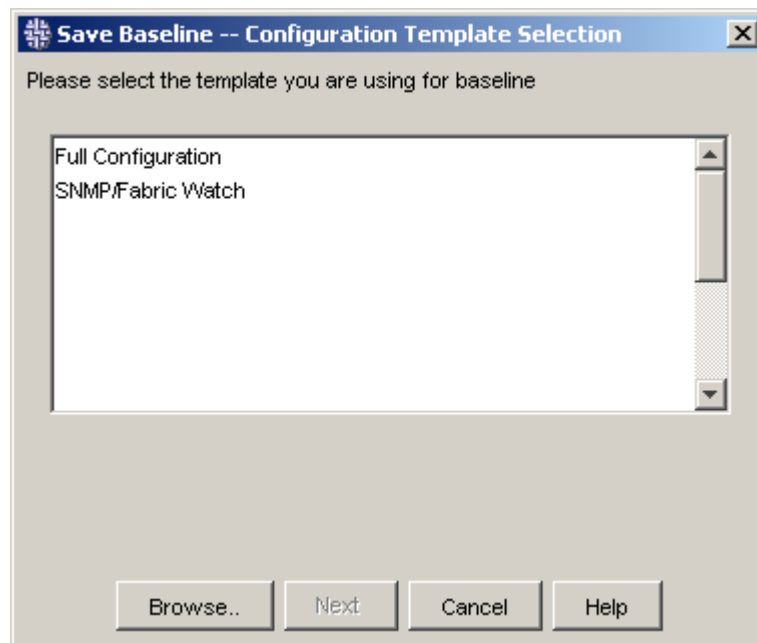


Figure 15: Description Change Results

The section Tag

Each **section** tag adds a section from the configuration file to the template. Sections appear in the configuration file as text in square brackets ([]). Section tags contain prefix tags.

In the example that follows, the **section** tag uses a **Boot Parameters** **value** attribute to add the Boot Parameters section of the configuration file to the display. It uses a **Boot Parameter** **text** attribute to identify the check box in the Save Baseline -- Parameter Selection dialog box. This **section** tag includes a **prefix** tag to add parameters to the section.

Example

```
<section value="Boot Parameters" text="boot parameters">
  <prefix ID="boot" text="Boot"/>
</section>
```

The results of this configuration appear in [Figure 16](#).

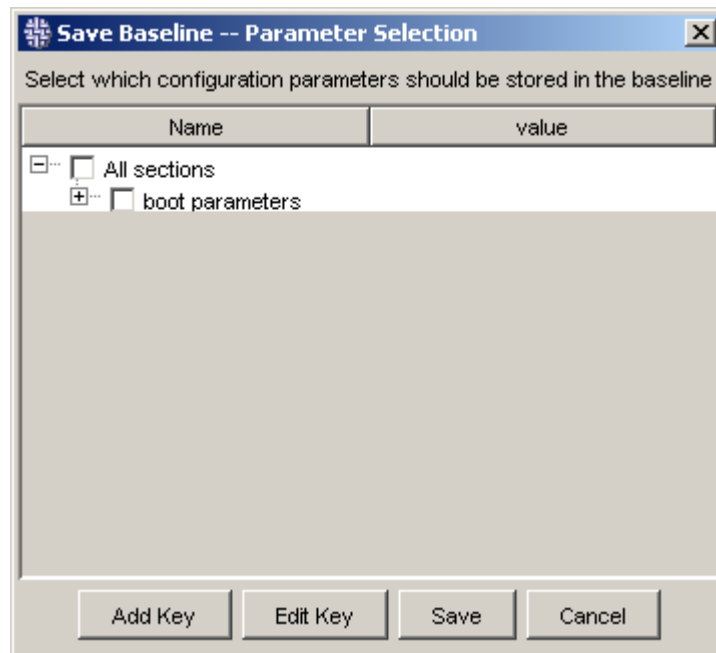


Figure 16: Section Change Results

The prefix Tag

The **prefix** tag adds parameters to the template. Every parameter in the configuration file includes a prefix before the first dot (.). Set the **ID** attribute of the prefix tag to add all configuration file parameters that use that prefix to the template. For instance, if you set the ID attribute to **route**, parameters such as route.delayReroute, route.embeddedPortBcast, and route.stickyRoutes appear in your template. Set the **text** attribute to define the text that accompanies the parameter in the Save Baseline -- Parameter Selection dialog box.

The example that follows adds all parameters in the configuration file that begin with **boot.** to the template.

Example

```
<prefix ID="boot" text="Boot"/>
```


The results of this configuration appear in [Figure 17](#).

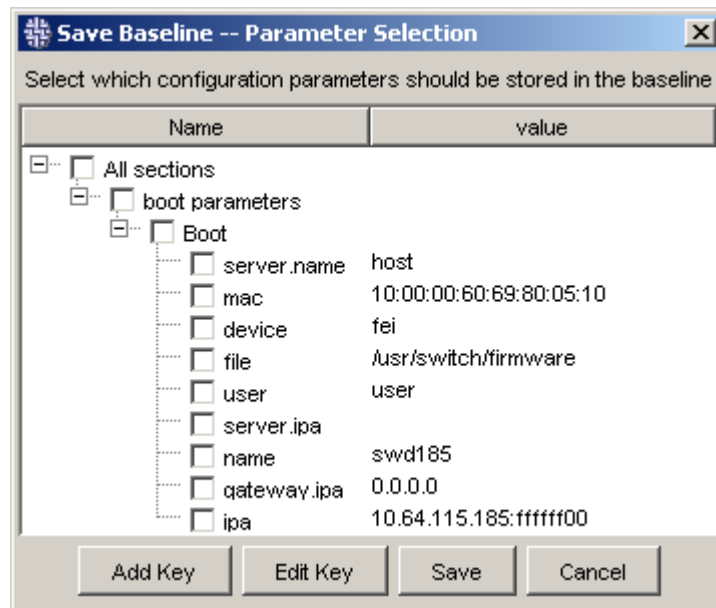


Figure 17: Prefix Change Results

Creating or Editing a Template

To create a custom baseline template:

1. Open `fullBaseLineTemplate.xml` in a text editor.

Note: When running Fabric Manager in a Windows environment, Notepad does not work for this task. To edit the XML document, you must open the file in WordPad or a similar application that recognizes carriage returns.

2. Edit the text that is displayed between the `<summary>` and `</summary>` tags to configure the template name that is displayed in the Save Baseline -- Configuration Template Selection dialog box.
3. Add or remove **section** tags to include or remove sections from the Save Baseline -- Parameter Selection dialog box.
4. Add or remove **prefix** tags to **section** tags to include or remove parameters from the Save Baseline -- Parameter Selection dialog box.

In each section, include only prefixes that appear in the analogous section in the configuration file.

5. Save the file to customize the existing file, or save the file in the same directory with a different file name to create a new configuration.

Fabric Merge Check

10

Perform a fabric merge check to determine whether two fabrics segment if you merge them. Fabric Manager provides the fabric merge check to compare various configuration elements of two fabrics before you connect those fabrics. Fabric Manager extracts copies of configuration elements from each fabric that can cause the fabric to segment and compares them in memory for inconsistency. Inconsistencies are displayed in the merge-check results window. Fabric Manager performs the following tests during a fabric merge check:

- Domain ID test
- TimeOutValue test
- Buffer-to-Buffer Credit test
- Disable Device Probe test
- Route Priority per Frame test
- Sequence Level Switching test
- Suppress Class F test
- Long Distance Mode test
- InterOp Mode test
- Data Field Size test
- VC Encoding test
- PID test
- Zoning test (runs only on non-secure fabrics)
- VC Priority test

The following tests run only in a secure fabric:

- Security test
- FCS policies test
- SCC policy test
- Version stamp test
- Management Server platform test

If the test is not applicable to the fabric, the test is not executed and Fabric Manager displays the message, `Test not applicable to subject fabrics`.

For example, if one or more fabrics are secure, the management server platform test and the zoning test are not executed and the message is displayed.

Comparing Fabrics for a Fabric Merge

You can check any two fabrics that you have discovered.

To perform a fabric merge check:

1. Log into the switches that you want to check. For more information, see [“Logging In to Multiple Devices Simultaneously”](#) on page 48.
2. From the **Tools** menu, select **Fabric Merge**. The Fabric Merge Check dialog box opens.
3. From each fabric pull-down menu, select one of the two fabrics that you want to merge and click **Check**. A **Merge Check Results** list displays and identifies the inconsistencies between the fabrics.

Note: If you run a fabric merge check between a secure fabric and a nonsecure fabric, the results of the Security, FCS policies, version stamp, and Management Server platform tests display the following message `Not applicable to subject fabrics`.

If the two zoning databases on the fabrics prevent the fabrics from merging, you are queried about launching the Zone Merge Manager tool. If you choose to do so, the Zone Merge Manager is launched and highlights in red all zoning conflicts between the two fabrics' zoning configurations. You can resolve the conflicts and apply the results to either of the fabrics in question.

After this process, you are returned to the Merge Check Results window, where, at the zoning test stage, it reports, `Merge Check Successful`, along with the results of the other tests. If you did not to enter the Zone Merge Manager, the zoning test would report `Operator cancelled zone merge - Merge Check Failed` for the zoning test, along with the results of all the other tests in the Merge Check Results window.

Licensing

11

Introduction

Note: Some of the following licenses are standard with HP switches and are activated.

Fabric Manager can display, store, load, and reload your license keys so that you do not lose them if your switch fails. With E-Licensing, you can request license keys online and install them with Fabric Manager.

Note: An Advanced Web Tools license must be installed on a switch for Fabric Manager to recognize the switch. All other licenses can be installed using Fabric Manager.

You can print license information about switches from the License Admin dialog box by clicking **Print**.

You must have an activated license (on each switch in the fabric) to use the following features:

Note: Only Trunking and Advanced Web Tools are supported by the MP Router.

- Full Fabric
- Extended Fabric
- Entry Fabric
- Fabric Watch
- Trunking
- Advanced Performance Monitoring
- Security
- QuickLoop
- Remote Switch
- Remote Fabric
- Advanced Zoning
- Advanced Web Tools

Exporting and Importing License Keys

Export license keys from healthy switches to a file so you can restore the licenses if switches fail. If for any reason you need to recover your license keys, import those keys from the file you created.

Exporting License Keys from Switches to a File

You can export the license keys of multiple switches to a single file. You can even export keys from different switches in different fabrics to one file. The file matches the license keys to the WWN of the appropriate switch so you can quickly and easily import the keys at any time.

To export license keys to a file:

1. Select **Tools > Licensing > Load from Switch**. The License Admin -- Switch Selection window is displayed.
2. Click the switches and/or fabrics with license keys that you want to export from the **SAN Elements** tab.
3. Click the right-pointing arrow to move elements that you selected into the right window and then click **OK**. The License Administration window is displayed. If you have not already logged in to the switches, Fabric Manager prompts you to do so.
4. Click the **Switch** tab and then click the **Export to File** button. The Export Licenses as an XML file dialog box opens.
5. Select a directory, enter a name for the file and click **Export**.



Caution: Do not open or manually edit this file.

Importing License Keys from a File to a Switch

If you need to restore license keys to a switch, import the keys that you saved to a file.

To import license keys from a file:

1. Select **Tools > Licensing > Import from File**. The Import License -- Select license file window is displayed.
2. Navigate to your license key file, select it, and click **Open**. The License Administration window is displayed.
3. Click the licenses that you want to download and click **Download to Switch**. Fabric Manager loads the licenses to the appropriate switches. If you have not already logged in to the switches, Fabric Manager prompts you to do so.

Removing a License Key from a Switch

To remove a license key and disable the functionality of a licensed feature:

1. Select **Tools > Licensing > Load from Switch**. The License Admin -- Switch Selection window is displayed.
2. Click the switches and fabrics with license keys that you want to remove from the **SAN Elements** tab.

3. Click the right-pointing arrow to move elements that you selected into the right most window and then click **OK**. The License Administration window is displayed.
4. Click the **Switch** tab.
5. Click the licenses that you want to remove and then click **Remove from Switch**.

Performing E-Licensing

E-Licensing provides users with the ability to acquire licenses online for switch-based software features. To use this feature, users need to have already purchased the licenses and obtained a transaction key in electronic form. Electronic transaction keys are provided as a file, typically delivered as an attachment to an e-mail.

Note: Not all fabric infrastructure providers support the delivery of electronic transaction keys; therefore, this feature may not be available to some users.

Obtaining Licenses from Transaction Keys

To obtain licenses from transaction keys:

1. Request a transaction key file from your switch supplier.
2. Download the transaction key file from your email to your client machine.
3. Log in to the switches for which you want to obtain a license. For more information, see [“Logging In to Multiple Devices Simultaneously”](#) on page 48.
4. Select **Tools > Licensing > Generate Licenses**. The Create License Request -- Select transaction key file or saved request dialog box opens.
5. Open the transaction key file. The License Request Administration window opens and displays all of the features available to you from the transaction key files that you opened.
6. Select one or more of the features in the **Feature Name** column.
7. Click **Select Switches**. Only switches already discovered by Fabric Manager display in the Switch Selection dialog box. You can select only as many switches as you have transaction keys per switch.
8. Click switches for which you want to obtain licenses in the **SAN Elements** tab and then click **OK**. If you have not already logged in to the switches, Fabric Manager prompts you to do so.
9. Do one of the following:
 - Click **Save Request** to save the License Request file in XML format and submit at a later time.
 - Click **Load TXN Key** to select another transaction key file or a saved License Request file.
 - Click **Submit** to submit the request. If you entered your email address in the request, you receive a record of licenses by e-mail.
 - Click **Reset** to remove any switches that you have entered in the **Switches** column and to reset the available quantity.

The License Administration window opens.

10. Click the **Obtained Licenses** tab. All the licenses that you obtained are displayed.
11. Click one or more licenses and then click **Download to Switch** to download the licenses to your switches.

To obtain the Security license, you must accept a license agreement.

Downloading Firmware

12

Perform a firmware download with Fabric Manager to concurrently download firmware to multiple switches and (optionally) reboot the switches simultaneously. Before you download firmware, verify that your task meets the following requirements:

- All switches that you choose to upgrade can run the firmware that you plan to download.
- All switches that you choose to simultaneously reboot reside on the same fabric.
- TCP/UDP Ports 20 and 21(FTP) must be accessible between the Fabric Manager server and each switch.

When you upgrade firmware from v3.0.0 or v4.0.0 to v3.1.0 or v4.1.0, any port name changes that you have made in Fabric Manager are lost; this ensures that multiple Fabric Manager clients that are simultaneously active during the firmware upgrade do not overwrite each other's port names.

When you download firmware to multiple switches at once and then reboot the switches simultaneously, you use less time than if you update your switches individually.

Note: The firmware download to multiple switches feature is not supported for MP Routers using Fabric Manager. If you attempt to download firmware on an MP Router using Fabric Manager, the Advanced Web Tools is launched. Refer to the *HP StorageWorks XPath OS Version 7.1.x Advanced Web Tools User Guide* for more information.

Performing a Firmware Download to Multiple Switches

To download firmware to multiple switches:

1. Log in to the switches that you want to upgrade. For more information, see [“Logging In to Multiple Devices Simultaneously”](#) on page 48.
2. From the **Tools** menu, select **Firmware download to switches**. The Firmware download to switches window opens; see [Figure 18](#).

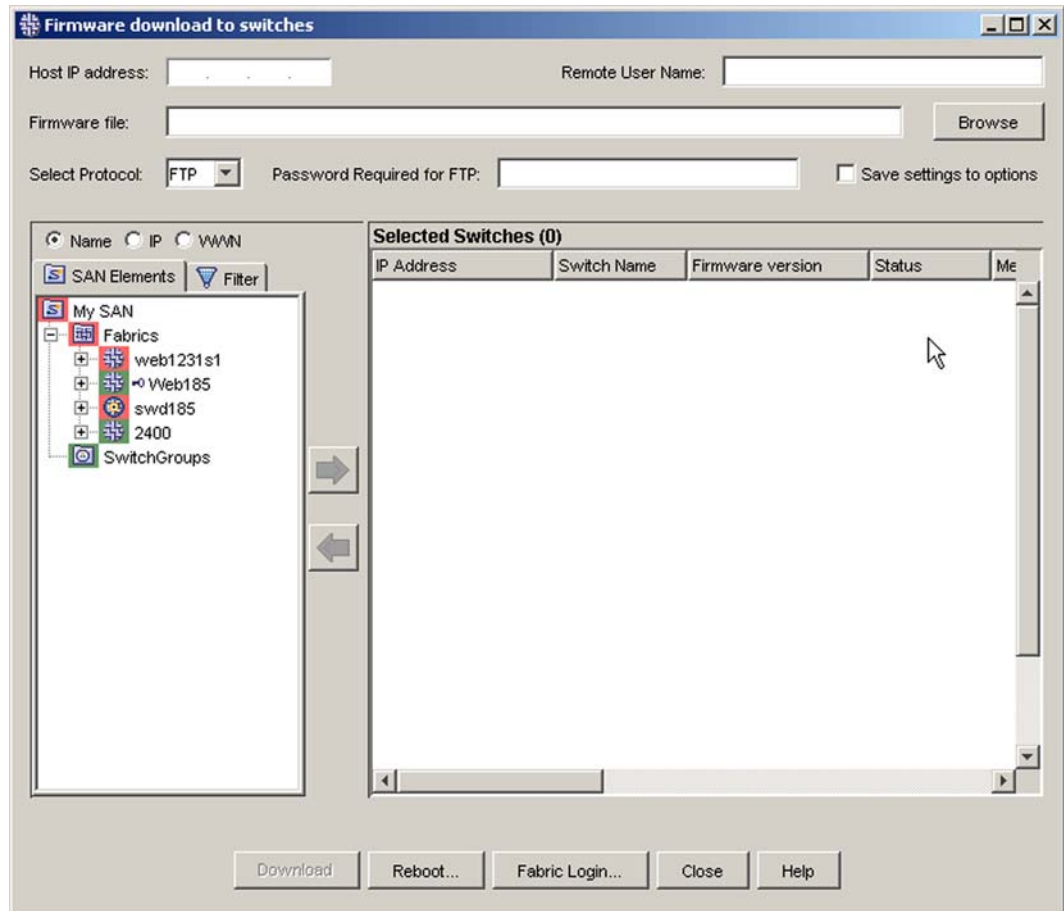


Figure 18: Firmware Download to Switches Window

3. In the **Host IP address** field, enter the IP address of the FTP server with the firmware file. If you have not configured file transfer options, check the **Save settings to options** check box to save your FTP settings as your file transfer options. For more information, see [“Configuring File Transfer Options”](#) on page 52.

Note: You must click **Download** to commit the file transfer options. If for any other reason you close this window, the file transfer options do not apply.

4. In the **Remote User Name** field, enter your user ID for the FTP server.
5. In the **Firmware file** field, enter the path and name of the firmware file (in UNIX format), or click **Browse** to navigate to the file.

6. If you are downloading firmware from a local Windows FTP host, ensure that the device designation (for example, C:) is not present and also that the filename contains forward slashes (/) rather than backslashes (\). If you enter the IP address first (see [step 3](#)) this occurs automatically.

Note: If Fabric OS v4.x is running, the filename includes an identifier for the hardware platform (for example, SWBD10). You must remove this from the filename.

7. From the **Select Protocol** pull-down menu, select **FTP**.
8. In the **Password Required for FTP** field, enter your password.
9. From the **SAN Elements** tab, select the switches that you want to upgrade and move them to the Selected Switches window. You can:
 - Navigate to a switch, click the switch, and then click the right-pointing arrow.
 - Click and drag a switch from the **SAN Elements** tab to the Selected Switches window.
 - Press and hold **Ctrl**, click multiple switches, and then click the right-pointing arrow.
 - Press and hold **Ctrl**, click multiple switches, and then click and drag the switches from the **SAN Elements** tab to the Selected Switches window.
 - Click and drag a fabric to the Selected Switches window to move or add all of the switches in that fabric to the Selected Switches window.

Note: You can perform a multiple-switch firmware download to a maximum of five switches running Fabric Manager version 4.0 and 4.1.0. If you want to download firmware to a dual-switch chassis, you need to select only one logical switch in a dual-switch chassis. Both switches are upgraded. If you add both of the logical switches in a chassis to the Selected Switches window, you receive an error prompt when you click **Download**.

10. Click **Download**. For switches running Fabric OS versions earlier than v4.0.
11. When the download completes, click **Reboot** to open the Sequenced Reboot window.

Note: If the switch loses network connectivity during the firmware download from Fabric Manager, the firmware download action times out after 25 minutes for switches running firmware v2.x or v3.x and after 80 minutes for switches running firmware v4.x.

No error message is returned when the firmware download process is interrupted.

Controlling Firmware Download Reboots

Switches running Fabric OS versions prior to v4.0 do not automatically reboot after you perform a firmware download. Fabric Manager gives you the opportunity to create a download sequence so you can control the order in which the switches reboot. For more information, see [“Performing a Sequenced Reboot”](#) on page 112.

Sequenced Reboots

13

With Fabric Manager, you can define groups of switches that reboot simultaneously, and then configure groups to reboot sequentially. Reboot groups let you simultaneously reboot switches that run the same firmware, serve the same function, reside in the same physical location, or share any other attribute by which you want to group them. [Table 19](#) defines the critical terms in this section.

Table 19: Sequenced Reboot Options

Term	Definition
Reboot group	A group of switches (from the same fabric) that reboot simultaneously.
Timeout	Occurrence where a fabric does not stabilize within the amount of time that you configure.
Stabilization	Occurrence where all WWNs of a fabric appear in the <code>fabricshow</code> command output.

Reboot groups consist of one or more switches from a single fabric. You cannot group switches from different fabrics. Any given switch can belong only to one reboot group.

Sequenced reboots give sections of your SAN an opportunity to reboot and stabilize before other switches in the fabric begin to reboot, which reduces the load of inter-switch traffic on the SAN.

Use the following reboot strategies to take full advantage of this feature:

- Simultaneously reboot switches that run the same firmware.
- Simultaneously reboot switches of the same model.
- Reboot the core switches of a fabric and then the edge switches.
- Reboot the backbone of a large SAN and then reboot other sections.
- Reboot distant physical locations sequentially.
- Simultaneously reboot MP Routers.

Creating a Reboot Group

To create a reboot group:

1. Select **Tools > Reboot > Create Reboot Sequence**. The Create or change reboot groups and sequence window is displayed.
2. Select a fabric from the **Select Fabric** menu.
3. Click **Create**. The Create reboot group dialog box opens.
4. In the Name of the **Reboot Group** field, enter a name for the group.
5. In the **Fabric Stabilization timeout** field, specify the amount of time for the fabric to stabilize.
6. Optional: In the **What to do if timeout occurs?** field, click one of the following buttons:
 - **Prompt** displays a prompt when a timeout occurs that asks you if you want to continue.
 - **Continue** continues the reboot sequence when a timeout occurs.
 - **Abort** terminates the reboot sequence when a timeout occurs.

If you do not make a selection in this field, the default selection is **Prompt**.

7. In the **Delay After Fabric Stabilization** field, enter the amount of time that must elapse before the next reboot in the sequence begins.

Fabric Manager considers a fabric stable when all WWNs appear in the `fabricshow` command output.

8. Click **OK**. Your reboot group is displayed in the Reboot Groups tree.

When your reboot group is displayed in the Reboot Groups tree, bracketed text is displayed next to the name of the group. The text in the brackets represents the fabric stabilization timeout duration, timeout option, and delay after fabric stabilization options that you configured.

Example

```
[ 1m, P, 2m ]
```

In this example, 1m identifies a stabilization timeout of one minute, P identifies that Fabric Manager prompts you if a timeout occurs, and 2m indicates that two minutes are to elapse before the next reboot in the sequence begins.

Assigning Switches to a Reboot Group

To assign switches to a reboot group:

1. Select **Tools > Reboot > Create Reboot Sequence**. The Create or change reboot groups and sequence window is displayed.
2. Select a fabric from the **Select Fabric** menu. The switches in that fabric display in the Unassigned Switches window.
3. Click the reboot group that you want to populate.
4. Click a switch that you want to add to the group, click the left-pointing arrow, and click **OK** to save the changes and apply them later. Click **Apply** to save the changes and apply them now.

To add multiple switches at once, press and hold **Ctrl** and click each switch that you want to add. Then click the left-pointing arrow.

Creating Single Switch Reboot Groups

Create a single switch group to account for individual switches that you have not assigned to a group. Single switch groups include these individual switches in the reboot sequence.

To create a single switch group:

1. Select **Tools > Reboot > Create Reboot Sequence**. The Create or change reboot groups and sequence window is displayed.
2. Select a fabric from the **Select Fabric** menu.
3. Select a switch from the Unassigned Switches window. To create multiple single-switch groups, select multiple switches. Each switch is made into its own group.
4. Click the **Create single switch groups** button. The Create single switch reboot groups dialog box opens.
5. Optional: In the **Name of the Reboot Group** field, enter a name for the groups. If you do not enter a name for the group, a default name is assigned in the Reboot *SwitchName* format, where *SwitchName* is the name of the switch.
6. In the **What to do if timeout occurs?** field, click one of the following radio buttons:
 - **Prompt** displays a prompt when a timeout occurs that asks you if you want to continue.
 - **Continue** continues the reboot sequence when a timeout occurs.
 - **Abort** terminates the reboot sequence when a timeout occurs.
7. In the **Delay After Fabric Stabilization** field, enter the amount of time that must elapse before the next reboot in the sequence.

Fabric Manager considers a fabric stable when all WWNs display in the `fabricshow` command output.

8. Click **OK**. Your reboot group is displayed in the Reboot Groups tree.

Performing a Sequenced Reboot

To set up a sequenced reboot:

1. Log in to the switches that you want to reboot. For more information, see “[Logging In to Multiple Devices Simultaneously](#)” on page 48.
2. From the **Tools > Reboot > Sequenced Reboot**. The Sequenced Reboot window is displayed.
3. Select a fabric from the **Select Fabric** pull-down menu.
4. In the **Reboot Groups** tab, click the group that you want to reboot first and then click the right-pointing arrow to add it to the Selected Switches window.
5. Repeat [step 4](#) to add additional groups in the order that you want them to reboot.
To re-arrange the order of the reboot sequence, click the up and down arrow keys in the Sequenced Reboot window.
6. Click **Fastboot** or **Reboot** to begin the sequenced reboot. Fabric Manager prompts you several times to be sure that you want to proceed. The prompt presents potential problems in your fabric. A message is displayed at the end of the reboot sequence to list successful and unsuccessful reboots.

Working with Switch and Port Groups

14

Fabric Manager allows you to create groups of SAN elements (either switches or ports) that you can monitor and manage as a group. The groups feature allows you to organize switches by function, switch type, firmware version, or any other criteria that you select. You can also create functional hierarchies of groups. Using groups simplifies management tremendously; you can log in all switches in a group simultaneously, download firmware on all group elements simultaneously, activate licenses on all group members simultaneously, and so on).

A switch can be in multiple groups at the same time. Groups are global across Fabric Manager. Fabric Manager users using the same server sees the same groups, and they can make changes to the groups. If you remove a switch from a fabric, the switch is also removed from any groups it was a member of.

When you look at a logical switch group in the Topology view, links disappear if the switches in this group are no longer in the **SAN Elements** tab in Fabric Manager.

There are many uses for creating Fabric Manager groups, including:

- Create groups of switch model types or firmware versions to expedite firmware downloads.
- Group switches by function to monitor switches that belong to different departments or that serve as a backbone to the SAN.
- Group switches by physical location to monitor fabrics in disparate locations.
- Group switches by SAN island to monitor or update individual islands.
- Group switches by redundancy so you can maintain half of a fabric while the other half continues to carry traffic.
- Nest fabrics to drill down to the source of a problem. For instance, if you create a switch group for a campus and then nest within that switch groups for departments, you can move down the hierarchy to determine the source of any status change.
- Create separate groups for monitoring and management to reduce unnecessary levels of nesting.
- Group ports by certain devices and hosts to more easily monitor those elements.
- Use groups to simplify the monitoring view of a large or complex fabric.

Creating Switch Groups

To create a group of switches:

1. Select **File > Groups > Edit Switch Groups**. The Edit Switch Groups dialog box opens.
2. Click the **SwitchGroups** icon in the right window.

The group that you create is displayed nested within the item that you click in this step. If you click an existing group instead of the **SwitchGroups** icon, your new group appears as a subgroup of that group. After you create a group, you can click and drag it to a new location in the hierarchy.

3. Click **Create**. The Create Group dialog box opens.
4. Enter a name for your group in the **Name** field and click **OK**.
5. Click the icon of the group that you created.
6. In the left most window, click the switch that you want to add to your group and then click the right-pointing arrow to add the switch to the group.

To add multiple switches at once, press and hold the **Ctrl** key as you click additional switches, or simply click and drag any node in the tree to add the switches from that node.

Click and drag switches directly from the left most window to the switch group to more quickly populate the group.

7. Click **OK** after you add switches to your group. The group is displayed in the **SAN Elements** tab under SwitchGroups.
8. To view the contents of the group, click the group.

Creating Port Groups

To create a group of ports:

1. Select **File > Groups > Edit Port Groups**. The Edit Port Groups dialog box opens.
2. Click the **PortGroups** icon in the right most window.

The group that you create is displayed nested within the item that you click in this step. If you click an existing group instead of the **PortGroups** icon, your new group appears as a subgroup of that group. After you create a group, you can click and drag it to a new location in the hierarchy.

3. Click **Create**. The Create Group dialog box opens.
4. Enter a name for your group in the **Name** field and click **OK**.
5. Click the icon of the group that you created.
6. This step is switch-type specific.
 - **Directors:** In the left most window, click the fabric, switch, card, and port that you want to add to your group. Then click the right-pointing arrow to add the port to the group.
 - **All other switches:** In the left most window, click the fabric, then the switch, then the port that you want to add to your group. Then click the right-pointing arrow to add the port to the group.

To add multiple ports at once, press and hold the **Ctrl** key as you click additional ports.

Click and drag ports directly from the left most window to the port group to more quickly populate the group.

7. Click **OK** when you have finished adding ports to your group. The group is displayed in the **SAN Elements** tab under PortGroups.
8. To view the contents of the group, click the group.

Editing a Switch or Port Group

To edit a switch or port group:

1. Select **File > Groups > Edit {Switch | Port} Groups**. The Edit {Switch | Port} Groups dialog box opens.
2. Select the switch group or port group that you want to edit from the right window.
3. Add members from one group to another by dragging to another group.
Delete members from a group by selecting the member and clicking **Delete** in the Edit Groups dialog box.
4. Click **OK**.

Deleting a Switch or Port Group

To delete a switch or port group:

1. Select **File > Groups > Edit {Switch | Port} Groups**. The Edit {Switch | Port} Groups dialog box opens.
2. In the right window, navigate to the group that you want to delete and click that group.
3. Click **Delete**.
You can also select the group you want to delete from the **SAN Elements** tab and press **Delete** on your keyboard to delete a group.
4. Click **OK**.

Managing Alerts

15

The Fabric Manager Alerts view makes it easy for you to see all of the alerts against any elements you are monitoring with Fabric Manager. The Alerts view lists detailed information about the alerts.

Unacknowledged and unresolved alert information is displayed in boldface type in the Alerts view. When a fabric is deleted from Fabric Manager, any alerts generated by the fabric or its member switches are deleted from the Fabric Manager database as well.

The following sections describe three types of Fabric Manager alerts:

- [“Switch Status Change Alerts”](#) on page 117
- [“Switch Unreachable Alerts”](#) on page 117
- [“Change Management Triggered Alerts”](#) on page 118

Switch Status Change Alerts

When a switch changes from the Healthy state to the Marginal state, or from the Healthy state to the Down state, an alert is created.

In the case where the switch status change reason is updated, but the switch status remains Marginal or Down, new alerts are not generated, but the original alert is updated with the new switch status change reason (in the **Description** column of Alerts view).

If the switch status changes between Marginal and Down, no new alerts are generated, but the original alert is updated with the new severity (**Severity** column of Alerts view) and switch status change reason (in the **Description** column of Alerts view).

If the switch status changes to a Healthy state from a Marginal or Down state, the original alert resolve status is set to resolved (a value of Yes in the **Resolve Status** field in the Alerts view).

Switch Unreachable Alerts

When a switch cannot be reached from the Fabric Manager server, an alert is created.

If the switch remains unreachable (as identified in the **Description** column of Alerts view), no new alerts are created. The original alert is updated with the latest unreachable time (identified in the **Last Occurrence Time** column of the Alerts view) until the alert is resolved by the switch becoming reachable by the Fabric Manager server. The alert can be resolved only after the switch is again reachable by the Fabric Manager server, or when the switch is deleted from the fabric or Fabric Manager, or when the fabric the switch belongs to is deleted from Fabric Manager.

Change Management Triggered Alerts

You can configure Change Management to trigger alerts for the following changes:

- ISL changes
- Switches added to or removed from the fabric
- Switch configuration changes
- Zoning changes
- Name server changes
- Firmware version changes
- Licenses added or removed from switches in the fabric
- Port status
- Device links
- Security mode enabled or disabled
- Security policy changes

If you have elected to receive alerts through the Change Management feature, any alerts generated on switches or fabrics defined in your profile during checks defined in your profile are also displayed in the Alerts view. After a Change Management triggered alert is reported in the Alerts view, the status of the alert is updated every time a scheduled Change Management check is run. If there is no change in the alert status, the original alert is updated with the latest unreachable time (identified in the **Last Occurrence Time** column of the Alerts view) until the alert is resolved. For Change Management alerts, if you change the baseline profile that is configured to trigger alerts, any alerts previously triggered by that defined baseline profile are set to a status of resolved. The switch status change reason for those alerts (in the **Description** column of Alerts view) is updated to indicate that it is resolved because of a baseline change.

For more information about Change Management, see [Chapter 6, “Change Management.”](#)

Identifying Switches and Fabrics with Alerts

Switches and fabrics with associated unacknowledged and unresolved alerts of Critical or Warning severity levels are easy to identify in the Fabric Manager GUI:

- Icons are displayed in the **SAN Elements** tab next to the switch or fabric icons for those switches and fabrics that have unacknowledged and unresolved alerts of Critical or Warning severity levels. If a switch has a Critical or Warning severity level alert, the appropriate icon is also displayed at the fabric level to which that switch belongs. The alert icons are shown below:
- Icons are displayed in the At-A-Glance windows (in the Overview view) next to the switch or fabric icons for those switches and fabrics that have unacknowledged and unresolved alerts of Critical or Warning severity levels.

The Alerts view displays all alerts for all switches and fabrics monitored by Fabric Manager.

Acknowledging Alerts

When you acknowledge an alert, the alert icons are not displayed in the **SAN Elements** tab and At-A-Glance windows in the Overview view. In addition, when you acknowledge an alert, your user name is displayed in the **Acknowledger** column of the Alerts view. This lets other Fabric Manager users on the same server know that you have already acknowledged the alert and are aware of the issue. Once an alert is acknowledged, it cannot be unacknowledged.

To acknowledge alerts:

1. Click a switch or fabric in the **SAN Elements** tab that has associated alerts.
2. Select **View > Alerts** or click **Alerts** on the View Selector bar. The Alerts view is displayed, listing all alerts for the switch or fabric you selected in the **SAN Elements** tab.
3. Click the row that lists the alert you want to acknowledge.
4. Click **Ack**. The **Acknowledge Status** column value is changed to Yes, the **Acknowledger** column value displays your user name, and the **Ack Time** column value displays the time that you acknowledged the alert. The alert icons displayed in the **SAN Elements** tab and At-A-Glance windows (in the Overview view) are no longer displayed.

Resolving Alerts

Fabric Manager alerts are automatically resolved when the issue is no longer there, or the baseline has changed so the alert is no longer valid. You cannot manually resolve alerts.

Deleting Alerts

Alerts must be deleted manually from the Alerts view. You can delete only alerts that have been resolved (those that have a Yes value in the **Resolve Status** column of the Alerts view).

To delete alerts:

1. Click a switch or fabric in the **SAN Elements** tab that has associated alerts.
2. Select **View > Alerts**, or click **Alerts** from the View Selector bar. The Alerts view is displayed, listing all alerts for the switch or fabric you selected in the **SAN Elements** tab.
3. Click the row that lists the alert you want to delete. You can delete only alerts that have been resolved (those that have a Yes value in the **Resolve Status** column of the Alerts view).
4. Click **Delete**. The alert is deleted, and removed from the Alerts view.

Call Home

16

The Call Home feature of Fabric Manager continuously monitors the status of switches and sends a call home email message to user-defined email addresses when a triggering condition occurs. Triggering conditions include the following:

- Switch status change to Marginal or Down
- Switch status remains Marginal or Down but the switch status reason changes
- Switch reboot
- Switch unreachable (experiences a complete loss of IP connectivity)

Call Home, when enabled, automatically sends an email alert notifying you about the trigger condition. The e-mail alert from Call Home includes the following information:

- Reason for call
- Brief description of failure
- Switches on which the event occurred (provides name, IP address for Ethernet and Fibre Channel, and WWN)
- Domain ID of the switch
- Switch type
- Factory serial number of the switch
- Supplier serial number of the switch
- Firmware version
- Switch status and state

The Call Home email alert contains an attachment that includes the following information:

- Detailed switch information
- One hundred most recent events from the event log
- Output from the `supportshow` command in a text file

You can configure Call Home to use an external executable to send out alerts when an event occurs.

The Fabric Manager server monitors the switches that you have discovered. You can use the Fabric Manager client to configure specific switches to monitor or to establish global Call Home functionality. Fabric Manager allows you to configure the Call Home feature using a wizard.

Configuring Call Home

Call Home configurations act independently of each other. No configuration ever impacts another configuration. You must configure notifications before you can configure Call Home. For instructions on configuring notifications, see [“Configuring Notification Parameters”](#) on page 53.

To configure Call Home:

1. Select **Tools > Call Home**. The Call Home window is displayed ([Figure 19](#)).

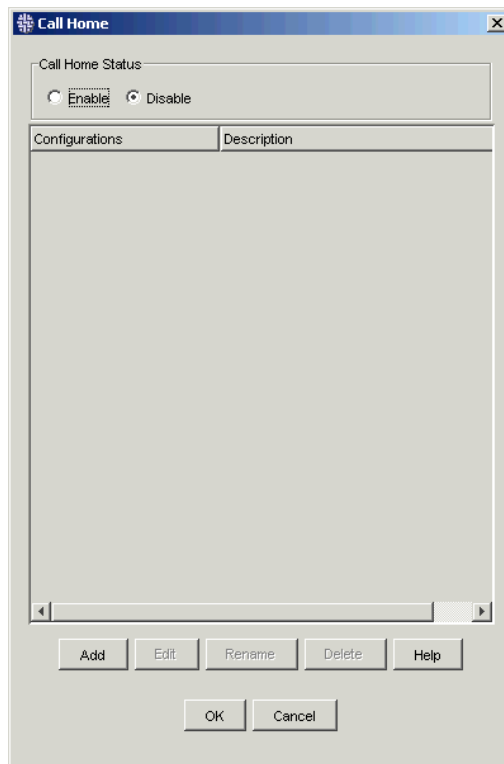


Figure 19: Call Home Window

2. Click **Add**. The Call Home Configuration wizard opens (see [Figure 20](#)).

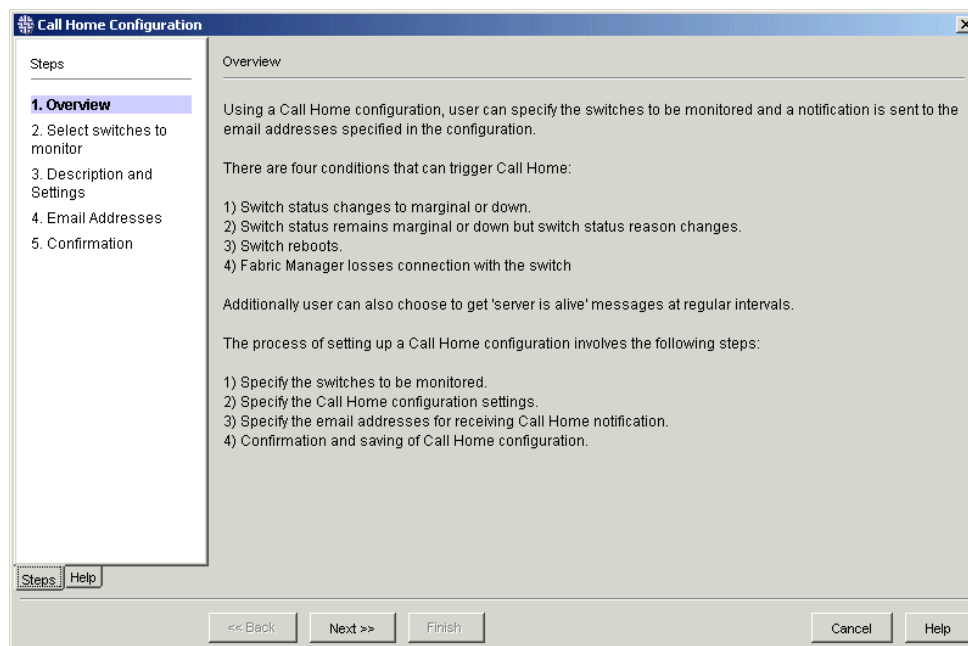


Figure 20: Call Home Configuration

3. Read the overview and click **Next**.
4. Click one or more switches on which to configure Call Home settings.
5. Click the right arrow button to move the switches to the **Selected Switches** list. If there is no login information set up for those switches, you are prompted to log in to the switches before proceeding.
6. Optional: Click **Include Support Show** to have Fabric Manager save a text file of the supportshow command output for each selected switch. The files are saved on the server; the location is included in the Call Home e-mail notification.
7. Click **Next**.
8. Enter a description for the Call Home configuration.
9. Enter the number of seconds that the server must fail to contact the switch before Call Home sends an unreachable e-mail alert. The duration default is 50 seconds. Fabric Manager does not accept a value less than 40 seconds.
10. Optional: Click the **Send “server is running” message** check box and enter the number of minutes for the interval at which you want to receive messages telling you that the server is running. The interval default is one minute. Fabric Manager does not accept a value less than 1 minute. These messages contain a list of switches in the configuration and informs you that Call Home continues to function properly.
11. Optional: In the **External Executable on Server** field, enter a path to an executable script that resides on the Fabric Manager server to run that script when Call Home sends an e-mail alert.
12. Click **Next**.
You must specify an e-mail address where Call Home e-mails are to be sent. If you do not want to get e-mail notifications, go to [step 14](#).
13. Optional: Click **Add**, enter an e-mail address, and then click **OK**.

14. Read the configured Call Home settings and click **Finish**. A dialog box opens, asking for the Call Home configuration name, if you are adding a new config only.
15. Click **OK** after you have entered the config name. A success message is displayed.
16. Click **OK**.
17. Click **Close** in the wizard to exit the wizard.

Editing Configurations

You can edit a Call Home configuration at any time. Any change that you make applies immediately after you commit the change.

To edit a Call Home configuration:

1. Select **Tools > Call Home**. The Call Home dialog box opens.
2. Click a configuration.
3. Click **Edit** to change the configuration settings. The Call Home Configuration wizard launches.
4. Make your changes. See “[Configuring Call Home](#)” on page 122 for details.
5. Optional: Click a configuration and then:
 - Click **Rename** to change the name the configuration.
 - Click **Delete** to delete the configuration.
6. Optional: you can also:
 - Click **Help** to launch online help.
 - Click **Add** to add a configuration.
7. Click **OK** to close the Call Home dialog box.

Globally Enabling or Disabling Call Home

To globally enable or disable Call Home:

1. Select **Tools > Call Home**.
2. Click **Enable** or **Disable**. This action processes on the server immediately.
3. Click **OK**.

Performance Monitoring

17

The Performance Monitoring feature is available only for switches running firmware versions 4.2.0c and later. If you have a switch or director running a firmware version earlier than 4.2.0c, the **Actions > Performance Monitor** menu option (and all suboptions) are unavailable.

Note: Performance Monitoring is not supported by the MP Router.

The Performance Monitoring feature in Fabric Manager allows you to see how much traffic a particular port is generating on a fabric through a period of time. The values for RX and TX for ports are retrieved at five-minute intervals (the interval cannot be changed) and are stored in a database. When you install Fabric Manager (server only, or both server and client), the database table schemas used for the performance monitoring features are copied to the following location (where you installed Fabric Manager):

```
Fabric Manager\ server\ db\ schema
```

You can run reports and generate graphs based on that information in Fabric Manager or on the information in an external tool, such as Crystal Reports. You can then save the reports and graphs on the Fabric Manager server.

Performance Monitor is enabled or disabled on an entire fabric, not on a switch or port basis. Before enabling Performance Monitor, creating graphs and reports, or creating templates, you must log in to the launch switch of the fabric. If you are not logged in to the switch, Fabric Manager prompts you to log in before proceeding.

Since performance data is collected over time, you should have Performance Monitoring enabled at all times so that information is constantly being saved. Since information is stored to the database, as you monitor larger fabrics using Performance Monitor, you should ensure you have ample database space.

If you delete a fabric, all performance monitoring data for that fabric is also deleted from the database.

Granularity

Granularity refers to the level of time-sample values that are used to generate a report. Fabric Manager stores a limited number of samples for each granularity, so every level of granularity is not available for all possible time ranges. For example, if you select a time range to be the last three days, the five-minute granularity level is not available.

The options for granularity are listed in [Table 20](#).

Table 20: Stored Samples for Granularity Options

Option	Stored Samples	Time Covered in Stored Samples
5 minutes	600	2 days and 2 hours
30 minutes	700	2 days and 2 hours, plus 12.5 days
2 hours	775	2 days and 2 hours, plus 12.5 days, plus 50 days
1 day	797	2 days and 2 hours, plus 12.5 days, plus 50 days, plus 732 days (rounded to 797 days)

There might be gaps in the stored data. Events that can cause gaps in data include:

- Authentication failures
- Switch not reachable
- Performance Monitoring feature turned off

Fabric Manager uses switch usernames and passwords to store data, so if the password is changed (resulting in an authentication failure) on a switch on which you have Performance Monitoring enabled, data collection fails (resulting in gap in stored data). An indicator is placed in the database instead, indicating that the data is missing due to an authentication error.

If a switch is unreachable, the performance data cannot be stored for the period of time that the switch is unavailable, resulting in a gap in stored data.

Similarly, when the performance monitoring feature is turned off, data is not gathered, resulting in a gap in stored data.

When data is not available for some of the points, when values are rolled up to the next time period value, the missing data is ignored.

Example

If five of the six five-minute values are 50 and the sixth value is missing, then:

N1= 50, N2= 50, N3=50, N4= 50, N5= 50, N6= NA, rolled up value for 30-minute entry=250 (because the N6 value is calculated as if it is a value of zero).

Reports

Fabric Manager allows you to create reports in two forms: reports and graphs. Graphs are discussed in “[Graphs](#)” on page 127. In Fabric Manager, you can create reports from templates, or you can customize reports. You can save, export, and print reports created in Fabric Manager.

Graphs

Fabric Manager allows you to create graphs of performance data (see [Figure 21](#)). There are no templates for performance monitor graphs, but you can create custom templates for graphs and custom graphs. Graphs can be saved and the information that is displayed can be edited.

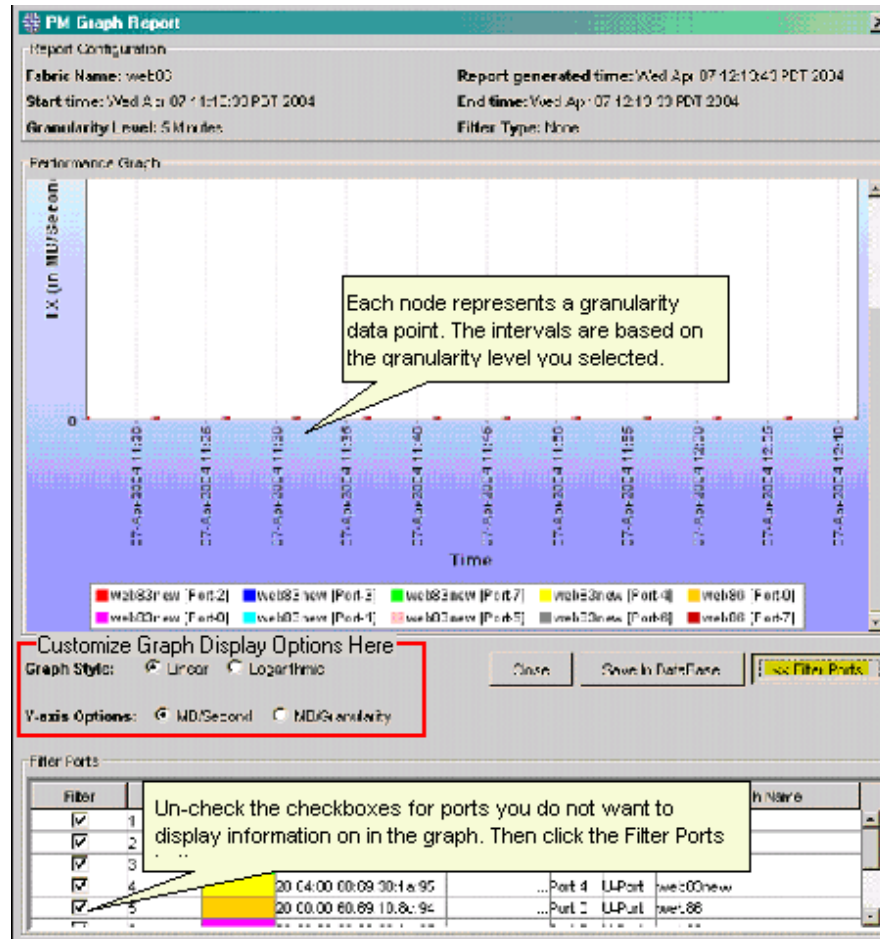


Figure 21: Using Performance Monitor Graphs

Templates

When you want to generate an ongoing report without a specified time interval, generate a performance monitor report from a template. Fabric Manager has six templates by default. The defaults templates are described in [Table 21](#).

Table 21: Default Performance Monitoring Report Templates

Report Type	Format Type	Time	Granularity	Filter
Top N of Ports (Aggregate Tx/Rx Traffic) over time T	Display (HTML)	Last 1 hour	5 minutes	None
Top N of Ports (Aggregate Tx/Rx Traffic) over time T	Display (HTML)	Last 30 minutes	5 minutes	None
Top N of Ports Receiving (RX) traffic over time T	Display (HTML)	Last 1 hour	5 minutes	None
Top N of Ports Receiving (RX) traffic over time T	Display (HTML)	Last 30 minutes	5 minutes	None
Top N of Ports Generating (TX) traffic over time	Display (HTML)	Last 1 hour	5 minutes	None
Top N of Ports Generating (TX) traffic over time	Display (HTML)	Last 30 minutes	5 minutes	None

You can create and save additional templates. For more information, see [“Creating Performance Monitor Report Templates”](#) on page 135.

Enabling Performance Monitoring

When you enable the performance monitor feature in Fabric Manager, you are enabling the port transaction information to be stored to a database. You must be logged in to the launch switch of a fabric for which you want to enable performance monitoring. If you are not already logged in to the launch switch, Fabric Manager prompts you to log in before proceeding.

To enable performance monitoring:

1. Click the launch switch in the **SAN Elements** tab.
2. Select **Actions > Performance Monitor > Config**. The Performance Monitoring Configuration dialog box opens.
3. Click **On** to store port transaction information to the database.
4. Click **Save**.

Disabling Performance Monitoring

When you disable the performance monitor feature in Fabric Manager, you prevent the port transaction information from being stored in a database. You must be logged in to the launch switch of a fabric for which you want to disable performance monitoring.

To disable performance monitoring:

1. Click the launch switch in the **SAN Elements** tab.
2. Select **Actions > Performance Monitor > Config**. The Performance Monitoring Configuration dialog box opens.
3. Click **Off** to stop storing port transaction information to the database.
4. Click **Save**.

Generating Custom Performance Monitor Reports

When you want to generate a one-time-use report or a report for a specified time frame, generate a custom performance monitor report. You can generate reports as text or in graphical format.

Performance Monitor Reports

To generate custom performance monitor reports (in a report format):

1. Click a switch in the **SAN Elements** tab.
2. Select **Actions > Performance Monitor > Reports > Generate Custom Reports**. The Generate Report dialog box opens ([Figure 22](#)).

Figure 22: Configuring Custom Performance Monitor Reports

3. Click **Report**.
4. Select a report type. The report types available are:
 - Top N of ports generating (Tx) traffic over time T
 - Top N of ports receiving (Rx) traffic over time T
 - Top N of ports (aggregate Tx/Rx) traffic over time T

5. Select a format type for the report. The format types are:
 - Display in HTML, which displays the report in HTML format.
 - Export in XML, which allows you to save the report to a file in XML format. You should save in XML format only if you want to export the data to another application.
 - Export in HTML, which allows you to save the report to a file in HTML format.
6. Type the number of results you want returned in the report in the **Top N** field. The number must be from 1 to 100.
7. Define the time range or interval:
 - To get information for a past amount of time, click **Last** and type a number. Select minutes, hours, or days.
 - To get information over a specific time interval, click **From Time** and enter values in the **from time** and **to time** fields.
8. Select the granularity time interval, which is the time sample interval. The available options are 5 minutes, 30 minutes, 2 hours, and 1 day. For more information on how granularity is calculated, see “[Granularity](#)” on page 125.
9. Select the ports for which you want to generate the report:
 - To consider all ports in the database with the specified granularity and time range, click **All**.
 - To report only device ports (F_Ports and L_Ports) in the database with the specified granularity and time range, click **Device Ports Only**.
 - To report only ISL ports (EX_Ports and E_Ports) in the database with the specified granularity and time range, click **ISL Ports Only**.
 - To select specific ports to filter, click **Advanced Port Selection** and then click **Select Ports**. The Advanced Port Selection dialog box opens (see [Figure 23](#)).

The **Available Switches** list shows all the switches available when the Performance Monitor Custom Report dialog box is opened. If another user has discovered or removed a fabric, switch, or port since then, it is not reflected in this list.

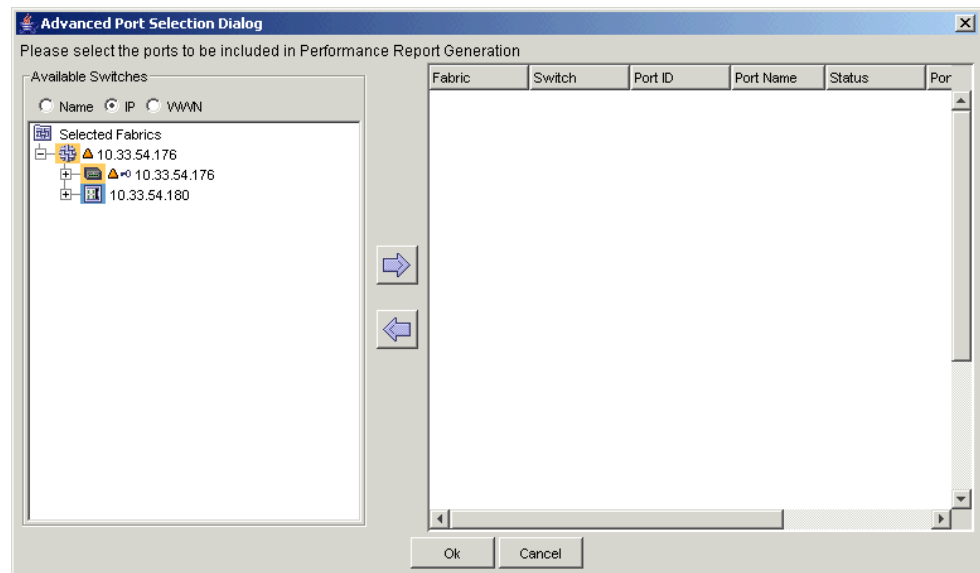


Figure 23: Selecting Ports for Custom Performance Monitor Reports

Click the ports you want to include in the report from the **Available Switches** list.
Click the right arrow to move them over and then click **OK**.

10. Click **OK** in the Generate Report dialog box.

If you selected a display in HTML format (see [step 5](#)), the report is displayed as shown in [Figure 24](#).

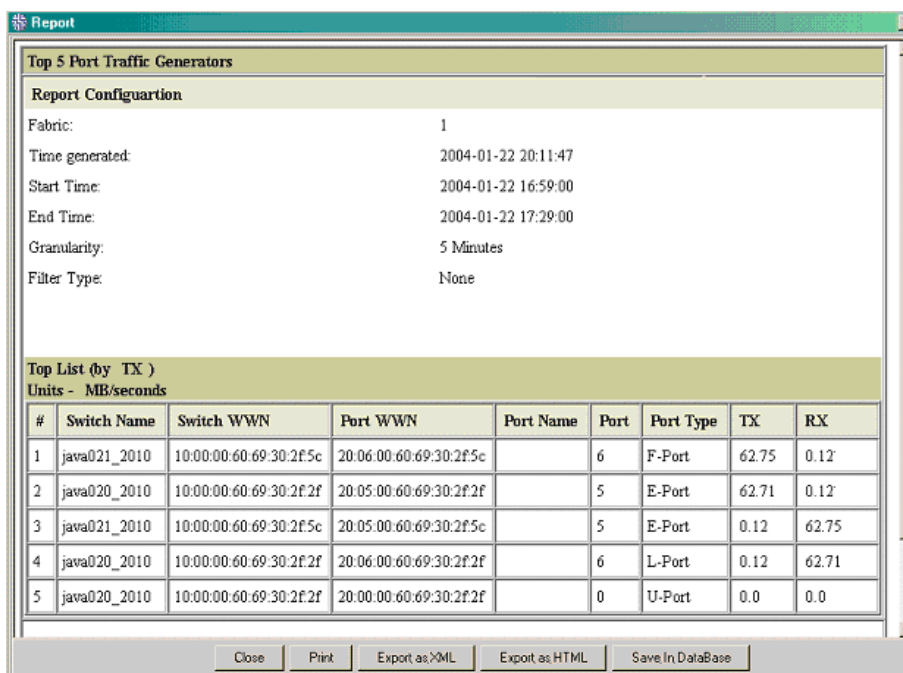


Figure 24: Performance Monitor Report Displayed in HTML Format

If there is no information matching the report criteria you selected, an information message is displayed stating No Performance statistics records were found matching the specified search criteria. Click **OK** in the information message to close it.

If you selected an export option (see [step 5](#)), a Save File dialog box opens. Navigate to the location where you want to save the file and then click **Save**.

At this point, you can do any of the following:

- Print the report, as described in “[Printing Performance Monitor Reports](#)” on page 136.
- Export the report in XML format, as described in “[Exporting Performance Monitor Reports](#)” on page 136.
- Export the report in HTML format, as described in “[Exporting Performance Monitor Reports](#)” on page 136.
Save the report, as described in “[Saving Performance Monitor Reports and Graphs](#)” on page 135.
- Export the report, as described in “[Exporting Performance Monitor Reports](#)” on page 136.

Generating Custom Performance Monitor Graphs

To generate custom performance monitor reports in a report format:

1. Click a switch in the **SAN Elements** tab.
2. Select **Actions > Performance Monitor > Reports > Generate Custom Reports**.

The Generate Report dialog box opens ([Figure 25](#)).

Figure 25: Configuring Custom Performance Monitor Graphs

3. Click **Graph**.
4. Select a report type. The report types available are:
 - Top N of ports generating (Tx) traffic over time T
 - Top N of ports receiving (Rx) traffic over time T
 - Top N of ports (aggregate Tx/Rx) traffic over time T
5. Type the number of results you want returned in the graph in the **Top N** field. The number must be from 1 through 20.
6. Define the time range or interval:
 - To get information for a past amount of time, click **Last** and type a number. Select minutes, hours, or days.
 - To get information over a specific time interval, click **From Time** and enter values in the **from time** and to **time fields**.

7. Select the granularity time interval, which is the time sample interval. The available options are 5 minutes, 30 minutes, 2 hours, and 1 day. For more information on how granularity is calculated, see [“Granularity”](#) on page 125.
8. Select the ports you want to include in the report:
 - To consider all ports, click **All**.
 - To report only device ports, click **Device Ports Only**.
 - To report only ISL ports, click **ISL Ports Only**.
 - To select particular ports to filter:
 - a. Click **Advanced Port Selection**.
 - b. Click **Select Ports**. The Advanced Port Selection dialog box opens (see [Figure 23](#) on page 130).
 - c. Click the ports you want to include in the report from the **Available Switches** list.
 - d. Click the right arrow to move them over and then click **OK**.
9. Click **OK** in the Generate Report dialog box.

If there is no information matching the report criteria you selected, an information message is displayed stating No Performance statistics records were found matching the specified search criteria. Click **OK** in the information message to close it.

A graph is displayed (see [Figure 26](#)).

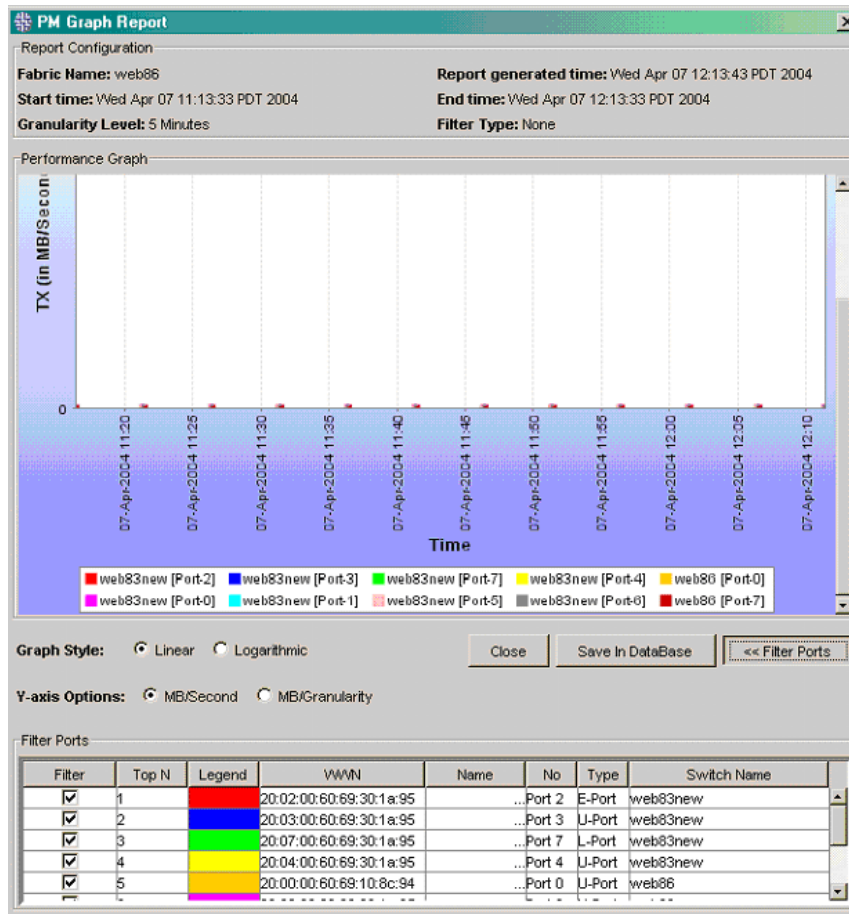


Figure 26: Performance Monitor Graph

At this point, you can do any of the following:

- Save the graph, as described in “[Saving Performance Monitor Reports and Graphs](#)” on page 135.
- Edit the graph view, as described in “[Editing Performance Monitor Graphs](#)” on page 138.

Generating Performance Monitor Reports from Saved Templates

To generate performance monitor reports from default or saved templates:

1. Click the launch switch in the **SAN Elements** tab.
2. Select **Tools > Performance Monitor > Reports > Generate From Templates**. The Generate From Templates dialog box opens.
3. To generate a report from a Fabric Manager template as is, or from a custom template you have already created as is, click the template and then click **OK**. The report is generated and displayed.

Creating Performance Monitor Report Templates

To create custom performance monitoring report templates:

1. Click the launch switch in the **SAN Elements** tab.
2. Select **Tools > Performance Monitor > Reports > Generate From Templates**. The Generate From Templates dialog box opens.
3. Click **New**. The Generate Report dialog box opens.
4. Click **Report** or **Graph**, depending on the type of representation you want for your report.
5. Select a report type. The available types available are:
 - Top N of ports generating (Tx) traffic over time T
 - Top N of ports receiving (Rx) traffic over time T
 - Top N of ports (aggregate Tx/Rx) traffic over time T
6. Select a format type for the report. The available formats are:
 - Display in HTML, which displays the report in HTML format.
 - Export in XML, which allows you to save the report to a file in XML format. You should save in XML format if you want to open and edit the information in Excel.
 - Export in HTML, which allows you to save the report to a file in HTML format.
7. Type the number of results you want returned in the report in the **Top N** field.
8. Type a number in the **Last time** field, and select minutes, hours, or days.
9. Select the granularity time interval, which is the time sample interval. The available options are 5 minutes, 30 minutes, 2 hours, and 1 day. For more information on how granularity is calculated, see [“Granularity”](#) on page 125.
10. Select the ports you want to include in the report:
 - To consider all ports, click **All**.
 - To report only device ports, click **Device Ports Only**.
 - To report only ISL ports, click **ISL Ports Only**.
11. Click **OK** in the Generate Template dialog box.

Saving Performance Monitor Reports and Graphs

To save performance monitor reports or graphs:

1. Generate a custom performance monitor report, or a report from a template, as described in the following sections:
 - [“Generating Custom Performance Monitor Reports”](#) on page 129
 - [“Creating Performance Monitor Report Templates”](#) on page 135
 - [“Generating Custom Performance Monitor Graphs”](#) on page 137
 - [“Generating Performance Monitor Graphs from Templates”](#) on page 138

The report or graph is displayed.

2. Click **Save in Database** to save the report or graph. The Save Report dialog box opens.
3. Type a file name for the report or graph.
4. Click **OK**.

Printing Performance Monitor Reports

To print performance monitor reports:

1. Generate a custom performance monitor report, or a report from a template, as described in
 - [“Generating Custom Performance Monitor Reports”](#) on page 129
 - [“Creating Performance Monitor Report Templates”](#) on page 135The report is displayed.
2. Click **Print** to print the report. The Print Report dialog box opens.
3. Select a printer.
4. Click **OK**.

Exporting Performance Monitor Reports

You can export performance monitor reports (not graphs) as HTML or XML and open them in external applications.

To export performance monitor reports:

1. Generate a custom performance monitor report, or a report from a template, as described in the following sections:
 - [“Generating Custom Performance Monitor Reports”](#) on page 129
 - [“Creating Performance Monitor Report Templates”](#) on page 135The report is displayed (see [Figure 24](#) on page 131).
2. Click **Export as XML** or **Export as HTML** to print the report. The Save dialog box opens.
3. Enter a file name.
4. Click **OK**.

Displaying Saved Performance Monitor Reports and Graphs

To display saved performance monitor reports and graphs:

1. Click the launch switch in the **SAN Elements** tab.
2. Select **Tools > Performance Monitor > Reports > Saved Reports**.
The Saved Reports dialog box opens.
3. Click the report or graph that you want to display.
4. Click **View**. The report or graph is displayed.

Deleting Performance Monitor Reports and Graphs

To delete performance monitor reports and graphs:

1. Click the launch switch in the **SAN Elements** tab.
2. Select **Tools > Performance Monitor > Reports > Saved Reports**. The Saved Reports dialog box opens.

3. Click the report or graph you want to delete.
4. Click **Delete**. The report or graph is deleted.

Generating Custom Performance Monitor Graphs

When you want to generate a one-time-use graph or a graph for a specified time frame, generate a custom performance monitor graph. To generate custom performance monitor graphs:

1. Click the launch switch in the **SAN Elements** tab.
2. Select **Tools > Performance Monitor > Reports > Generate Custom Reports**. The Generate Report dialog box opens.
3. Click **Graph**.
4. Select a report type. The available report types are:
 - Top N of ports generating (Tx) traffic over time T
 - Top N of ports receiving (Rx) traffic over time T
 - Top N of ports (aggregate Tx/Rx) traffic over time T
5. Type the number of results you want returned in the report in the **Top N** field.
6. Specify the time range or interval:
 - To get information for a past amount of time, click **Last** and type a number. Select minutes, hours, or days.
 - To get information over a specific time interval, click **From Time** and enter values in the **from time** and **to time** fields.
7. Select the granularity time interval, which is the time sample interval. The available options are 5 minutes, 30 minutes, 2 hours, and 1 day. For more information on how the granularity is calculated, see “[Granularity](#)” on page 125.
8. Select the ports to include in the report:
 - To consider all ports, click **All**.
 - To report only device ports, click **Device Ports Only**.
 - To report only ISL ports, click **ISL Ports Only**.
 - To select specific ports to filter, click **Advanced Port Selection** and then click **Select Ports**. The Advanced Port Selection dialog box opens.
 - a. Click the ports you want to include in the report from the **Available Switches** list.
 - b. Click the right arrow to move them over and then click **OK**.
9. Click **OK**. The report is displayed. You can now do either of the following:
 - Print the graph by clicking **Print**.
 - Save the graph by clicking **Save in Database**.

Generating Performance Monitor Graphs from Templates

When you want to generate a graph without a specified time interval, generate a performance monitor graph from a template. To generate a performance monitor graph from a template:

1. Click the launch switch in the **SAN Elements** tab.
2. Select **Tools > Performance Monitor > Reports > Generate From Templates**. The Generate From Templates dialog box opens.
3. To generate a graph from a Fabric Manager template as is, or from a custom template you created as is, click the template and then click **OK**. The graph is generated and displayed. You do not need to continue with this procedure.

To generate a graph from a template without specifying a time interval or filtering, click **New**. The Generate Report dialog box opens.

4. Click **Graph**.
5. Select a report type. The available report types are:
 - Top N of ports generating (Tx) traffic over time T
 - Top N of ports receiving (Rx) traffic over time T
 - Top N of ports (aggregate Tx/Rx) traffic over time T
6. Type the number of results you want returned in the graph in the **Top N** field. No more than 20 results can be reported in the graph.
7. Click **OK**. The graph is displayed. You can now do any of the following:
 - Display the graph in linear format by clicking **Linear**.
 - Display the graph in logarithmic format by clicking **Logarithmic**.
 - Filter out specific port information so it is not displayed in the graph by clicking **Filter Ports**.
 - Uncheck the port from the list to remove the information about that port from the graph.
 - Print the report by clicking **Print**.
 - Save the report by clicking **Save in Database**. For more information, see [“Saving Performance Monitor Reports and Graphs”](#) on page 135.

Editing Performance Monitor Graphs

You can customize the performance monitor graphs by:

- Displaying the graph in either a linear or logarithmic format
- Selecting the Y-axis to display MB/Second or MB/granularity
- Filtering ports

To change graph format:

1. Create a Performance Monitor graph, as described in “[Generating Custom Performance Monitor Graphs](#)” on page 132 or “[Generating Performance Monitor Graphs from Templates](#)” on page 138.
2. Display the graph (see [Figure 26](#) on page 134).
3. Click **Linear** to display the graph as a linear graph or **Logarithmic** to display the graph as a logarithmic graph.

To change the Y-axis values:

1. Create a Performance Monitor graph, as described in “[Generating Custom Performance Monitor Graphs](#)” on page 132 or “[Generating Performance Monitor Graphs from Templates](#)” on page 138.
2. Display the graph (see [Figure 26](#) on page 134).
3. Click **MB/Second** to display MB/second values on the Y-axis, or click **MB/Granularity** to display MB/granularity on the Y-axis.

To display information only for selected ports:

1. Create a Performance Monitor graph, as described in “[Generating Custom Performance Monitor Graphs](#)” on page 132 or “[Generating Performance Monitor Graphs from Templates](#)” on page 138.
2. Display the graph (see [Figure 26](#) on page 134).
A list of ports for which information is displayed is included in the graph report. To display only a subset of port information in the graph, you can filter them out. A selected check box means the information for that port is displayed in the graph.
3. To filter port information out of the graph, click the check box in the **Filter** column for the port you do not want to include in the graph. Repeat this step for as many ports as you want to filter out.
4. Click **Filter Ports**.

Displaying Performance Monitor XML Reports in External Applications

When you elect to export performance monitor reports in XML format, an `xslt` file (stylesheet) is also saved with the XML file. The `xslt` file can be used to translate the XML file into an Excel spreadsheet (or other software applications that allow you to open XML file types). You can then edit the information in the spreadsheet.

You do not need to use the `xslt` file provided by Fabric Manager, or any `xslt` file; however, if you do not use a stylesheet, the translated information is not very useful.

The following procedure uses Excel 2000 as a sample application in which you can open the XML file to manipulate the performance monitor data. There are also other applications in which XML files can be opened.

To open a Performance Monitor XML report in Excel:

1. Launch Excel 2002 (or later).
2. Select **File > Open**. The Open dialog box opens.

3. Navigate to the XML file, and click **Open**. The Import XML dialog box opens, asking you if you would like to open a stylesheet.
4. Click **Open the file without applying a stylesheet** (not recommended) or click **Open the file with the following stylesheet applied**.

If you clicked **Open the file without applying a stylesheet**, the information is displayed in an Excel spreadsheet without the formatting.

If you clicked **Open the file with the following stylesheet applied**, the `xslt` file created by Fabric Manager is the default selected file. You can either use that file, or navigate to another stylesheet of your own. Click **OK** to display the information in an Excel spreadsheet.

Using Fabric Manager With the MP Router

18

An MP Router running XPath OS v7.1.x can run a software application that enables you to share devices between two more fabrics using that switch to connect to the fabrics. The MP Router has a new port type called EX_Port. The EX_Port provides the connectivity between an edge fabric and a backbone fabric (see [Figure 27](#)).

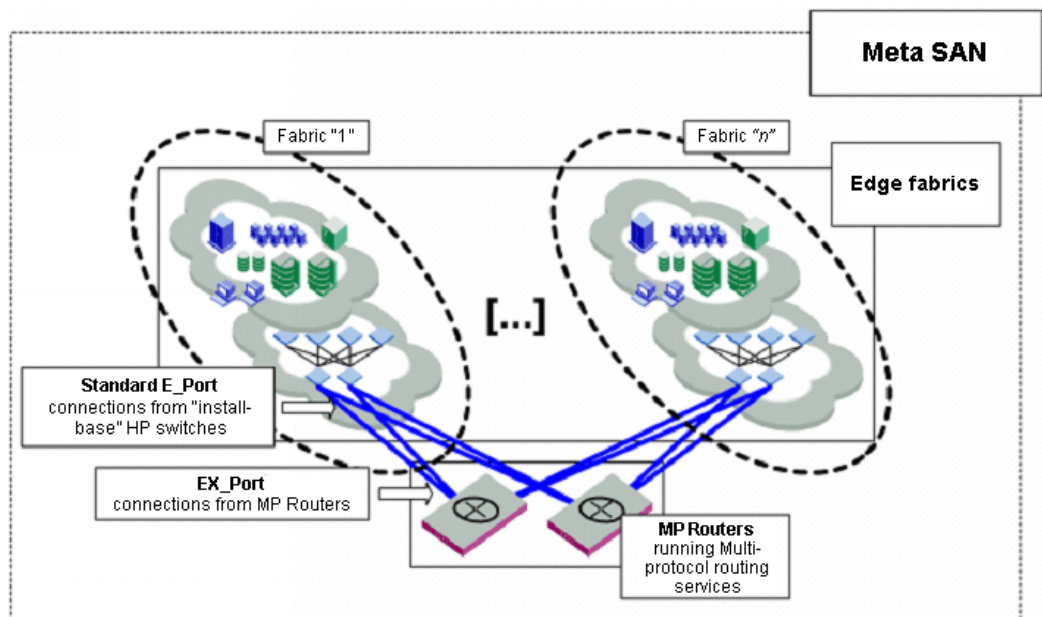


Figure 27: Sample Meta SAN Including MP Routers

Fabric Manager scans all switches discovered. Any switches running XPath OS firmware are considered MP Router-capable. If an EX_Port is configured for that switch, the switch is MP Router enabled. Switches that are MP Router-capable and MP Router enabled have special icons associated with them in the **SAN Elements** tab and At-A-Glance windows in the Overview view. Fabric Manager allows you to manage MP Routers and EX_Ports. The EX_Ports are displayed in all applicable Fabric Manager views including:

- Device Ports view
- Overview view
- Topology view

Sharing Devices Between Fabrics

You can share devices between fabrics without merging them together with the use of an MP Router. Fabric Manager allows you to set up the shared devices easily with the use of the Share Devices wizard. Using the wizard, you must first select the devices you want to share; the wizard then creates a logical SAN.

Using Fabric Manager, you can view and monitor information about all of the fabrics connected through the router in one place. Fabric Manager allows you to monitor FCR and EX port information.

To share devices between fabrics:

1. Select **Tools > Share Devices**. The FC Router- Share Devices [Create New LSAN] wizard launches.
2. Read the overview information and then click **Next**.
3. The Select Devices to Share dialog box opens (Figure 28).

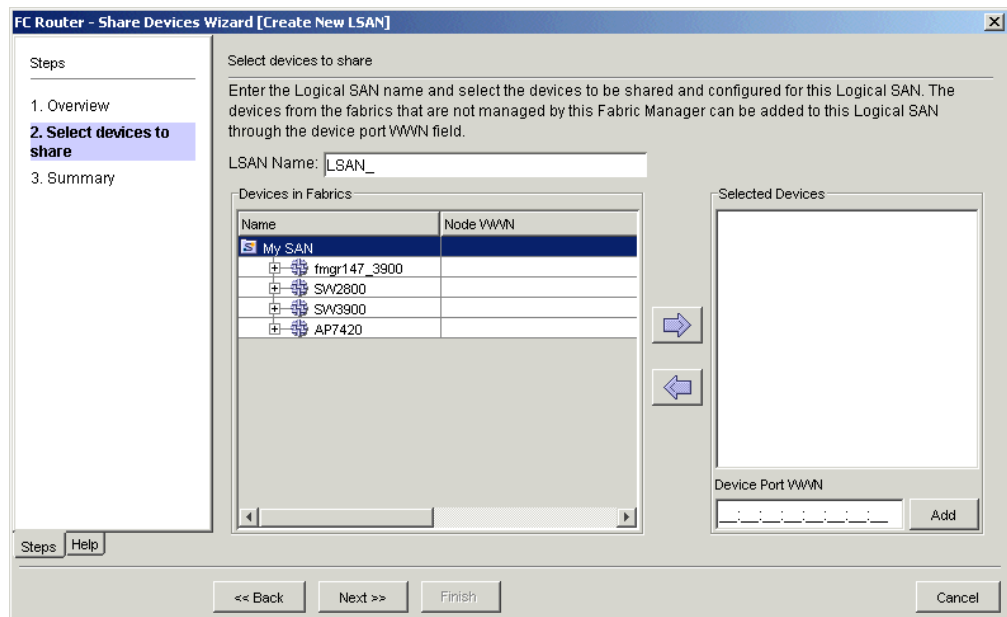


Figure 28: Selecting Devices to Share Dialog

4. Enter a name for the logical SAN (LSAN).
5. Click the devices you want to share from the **Devices in Fabrics** list.
You must select at least two devices from two different fabrics. If the devices are not displayed in the list, enter the device port WWN in the field below the **Selected Devices** list and click **Add**.
6. Click the right arrow to move the devices to the **Selected Devices** list.
7. Click **Next**. A summary displays the devices that are being shared in the new LSAN.
8. Read the summary. If something is incorrect, click **Back** to correct it. If everything is correct, click **Finish**.

Connecting Edge Fabrics

Fabric Manager allows you to connect edge fabrics to each other. To connect edge fabrics:

1. Click a switch in the **SAN Elements** tab that you want to connect to an MP Router.
2. Select **Actions > FC Router Configuration**. The FC Router- Connect Edge Fabrics wizard launches.
3. Read the information and then click **Next**. The Select FC Router dialog box opens (see [Figure 29](#)).

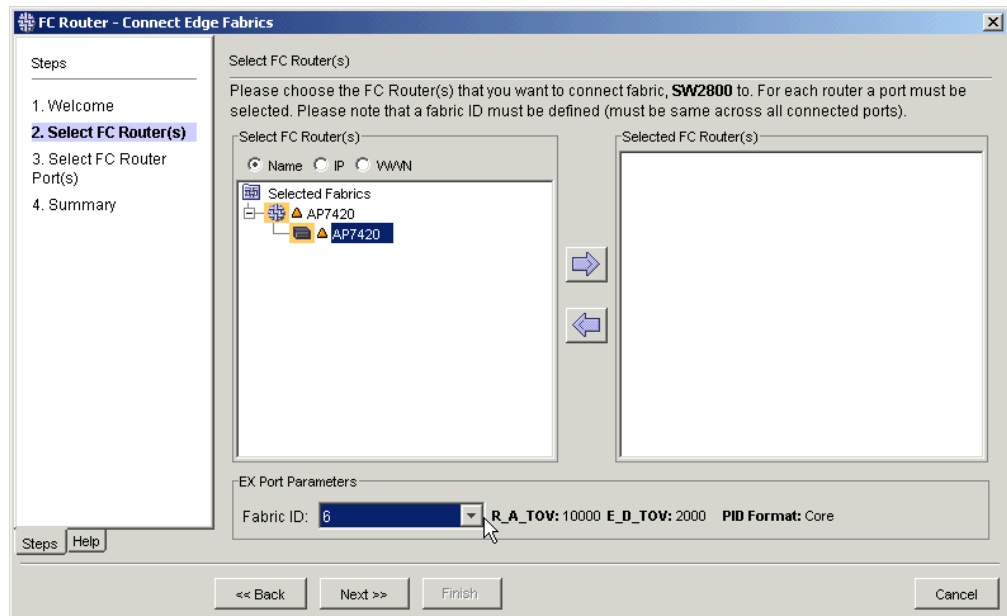


Figure 29: Select FC Router

4. Click one or more MP Routers that you want to connect to the first edge fabric.
5. Click the right arrow button to move them to the selected **FC Routers** list.
6. Select a Fabric ID for the EX port.
7. Click **Next**. The Select FC Router Ports dialog box opens.
8. Click the FC Router/port number that the first edge fabric is connected to.
9. Click **Next**. A summary displays the ports and routers you have configured to be edge fabrics.
10. Read the summary. If everything is correct, click **Finish**. A confirmation is displayed stating that the FC Router configuration might take a few minutes to complete.
11. Click **Yes** to complete the configuration process. An information message informs you that the configuration completed successfully, and that you should physically connect the selected edge fabrics to the FCR switches.
12. Click **OK**.
13. Click **Close** in the summary screen to exit.

Displaying Logical SANs

The Fabric Manager LSAN view displays information about the Logical SANs you are monitoring. The view includes information on each device defined in the LSAN as well. For more information, see [LSAN View](#).

FDMI-Capable HBA Firmware Download

19

Fabric Manager supports up to 50 firmware downloads to multiple HBAs simultaneously.

Currently, Emulex is the only vendor supporting FDMI for their HBA. Emulex has drivers for Windows 2000, Windows 2003, and Solaris. Fabric Manager supports only the Emulex HBA with the following drivers for the FDMI-based firmware downloads:

- Miniport Driver 5-5.02a3 (Windows 2000), Firmware 3.92A2
- Miniport Driver 5-1.02a3 (Windows 2000), Firmware 3.92A2
- Full Port Driver 5-2.22a8 (Windows 2000 and 2003), Firmware 3.9.2A2
- Solaris driver for Sparc systems version 6.00g, Firmware 3.92A2 (`lpfc.conf` must have `fdmi-on` option set to 1 to turn on FDMI)

FDMI-capable HBAs must be connected to an FDMI-capable switch to get the FDMI functionality.

FDMI is disabled by default on the Emulex HBA. You must enable FDMI by using either the `elxcfg` or `lputil` tool.

Downloading Firmware to an HBA



Caution: During a firmware download to an HBA, if you reboot the switch to which the HBA is attached, or reboot the host to which the HBA is attached, the firmware in the HBA flash can become corrupted, the HBA flash can become corrupted, and the HBA is not able to log back in to the switch or respond to the query from the switch.

Neither Fabric Manager nor the switch can see the HBA, and it drops out of the **Name Server** list. In this case, the solution is to use HBAnyware on the attached host and reload the firmware on the HBA.

To download firmware to one or more HBAs:

1. Log in to a switch (or switches) with version 3.1.0 or 4.1.0 firmware or later loaded and FDMI-capable HBAs connected to or them. For more information, see “[Logging In to Multiple Devices Simultaneously](#)” on page 48.
2. Select **Tools > Firmware download to HBAs**. The Firmware download to HBAs window is displayed.

3. In the **Host IP address** field, enter the IP address of the FTP server with the firmware file.
The IP address is displayed automatically if you have already configured file transfer options. For more information, see “[Configuring File Transfer Options](#)” on page 52.
If you have not configured file transfer options, click the **Save settings to options** check box to save your FTP settings as your file transfer options.
4. In the **User Name** field, enter your user ID for the FTP server.
5. In the **Firmware file** field, enter the path and name of the firmware file (in UNIX format) or click **Browse** to navigate to the file.
Clicking Browse overrides the current settings for host IP address, user name, and password. The information defaults to the current host system from which the Fabric Manager application is executed.
6. In the **Password** field, enter your password.
7. From the **SAN Elements** tab, select the HBAs that you want to upgrade and move them to the Selected HBAs window. You can:
 - Navigate to an HBA, click the HBA, and click the right-pointing arrow.
 - Drag an HBA from the **SAN Elements** tab to the Selected HBAs window.
 - Press **Ctrl** while clicking multiple HBAs and click the right-pointing arrow.
 - Press **Ctrl**, while clicking multiple HBAs and drag the HBAs from the **SAN Elements** tab to the Selected HBAs window.
 - Drag a fabric to the Selected HBAs window to add all of the HBAs in that fabric to the Selected HBAs window.



Caution: Simultaneous firmware downloads to one or more HBAs on the same host from multiple Fabric Manager clients is not supported and may permanently corrupt the firmware on the HBAs, causing them to be unusable.

Non-FDMI capable HBAs appear with a grey background.

If Fabric Manager detects that a device is no longer in the Name Server, the device is displayed with a grey background in the Firmware Download to HBAs window until the device logs in to the Name Server again.

8. Click the **Download** button to begin the firmware download. Fabric Manager prompts you with a confirmation dialog box.
9. Click **OK** to proceed or **Cancel** to abort. Fabric Manager provides a report of successful and unsuccessful downloads.

Note: Click **Refresh FDMI** to refresh FDMI information available in the Firmware Download to the HBA window for the selected HBAs.

Security

20

Fabric Manager allows you to create a secure fabric. You can define the **Fabric Configuration Servers (FCS) switch** list, set new passwords and define new policies for various accounts for FCS and non-FCS switches, and reboot the switches running firmware versions 4.2.x or 3.2.0 or earlier.

Before you can enable secure mode, you must define the **FCS switches** list. Next, you must set the passwords for different accounts. Then, you have the option of creating a set of policies and defining Security Levels (High, Medium, Low, and Custom) while enabling secure mode. Configuring switch permissions is a fabric-wide operation, not a switch-by-switch operation, and applies only to secure switches.

You can configure policy settings later as well by using the Policy Editor in Fabric Manager (see [Figure 30](#)). If you do not define policies, the FCS and SCC policies are created by default and the security setting is set to Low by default.

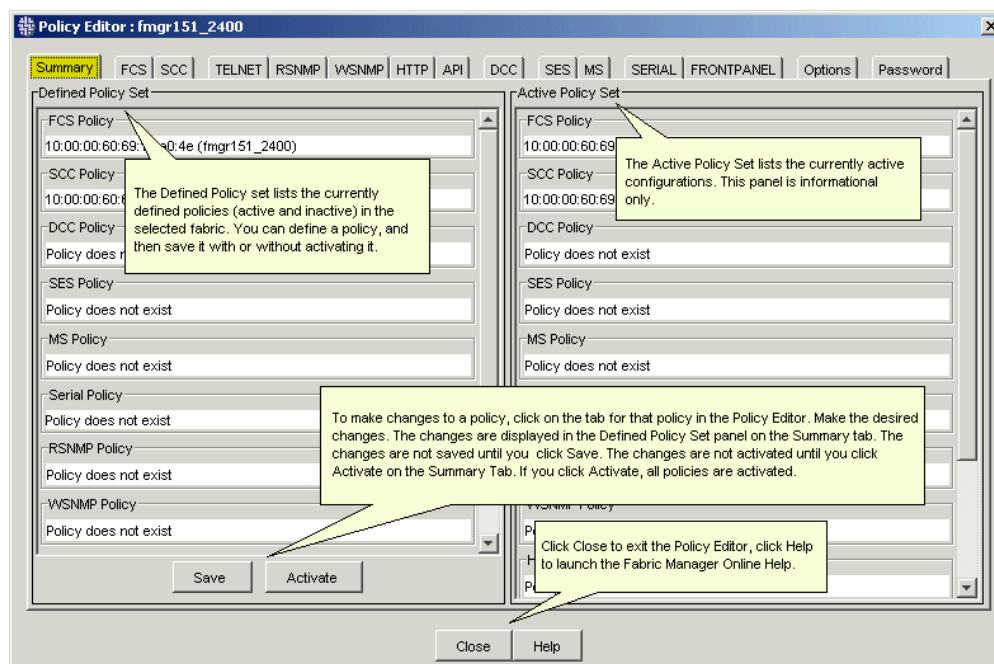


Figure 30: Policy Editor

To enable secure mode on a fabric, you must have a security license, a zoning license, and certificates installed on the switch.

Note: The enable/disable secure more option is applicable only to switches running firmware versions later than 4.2.0x. If you have a switch or director running firmware version 4.2.0x or earlier, selecting this menu options displays an error message.

The API, HTTP, RSNMP, WSNMP, and Telnet Policies require an IP address of a management workstation.

If you create either empty policies in the serial, Telnet, HTTP, and API policies simultaneously or policies without Fabric Manager Client/Server IP addresses, you can no longer manage security and are no longer be able to manage the switch.

Security Levels

The set of security policies is divided into four security levels; high, medium, low and custom. As part of enabling the secure mode in Fabric Manager, you can select security policy settings, as described in [Table 22](#), [Table 23](#), and [Table 24](#). If you do not select security policy settings, the low security level is applied to the switch.

Table 22: High Security-Level Settings Per Policy

Policy Name	Policy Exists	Description
SCC	Yes	Policy is created only with the current switches in the fabric.
DCC	Yes	Policy is created only with the currently connected/online devices in fabric.
API	Yes	Policy is created with the Fabric Manager server and all client IP addresses.
HTTP	Yes	Policy is created with the Fabric Manager server and all client IP addresses.
Telnet	Yes	Policy is created with the Fabric Manager server and all client IP addresses.
SNMP	Yes	An empty policy is created, which disables access by anyone.
Management Server	Yes	An empty policy is created, which disables access by anyone.
Serial Port	Yes	An empty policy is created, which disables access by anyone.
Front Panel	Yes	An empty policy is created, which disables access by anyone.

Table 23: Medium Security-Level Settings Per Policy

Policy Name	Policy Exists	Description
SCC	Yes	Policy is created only with the current switches in the fabric.
DCC	Yes	Policy is created only with the currently connected/online devices in fabric.
API	Yes	Policy is created with the Fabric Manager server and all client IP addresses.
HTTP	Yes	Policy is created with the Fabric Manager server and all client IP addresses.
Telnet	Yes	Policy is created with the Fabric Manager server and all client IP addresses.
SNMP	No	No policy is created; everyone is allowed access.
Management Server	No	No policy is created; everyone is allowed access.
Serial Port	No	No policy is created; everyone is allowed access.
Front Panel	No	No policy is created; everyone is allowed access.

Table 24: Low Security-Level Settings Per Policy

Policy Name	Policy Exists	Description
SCC	Yes	Policy is created only with the current switches in the fabric.
DCC	No	No policy is created; everyone is allowed access.
API	No	No policy is created; everyone is allowed access.
HTTP	No	No policy is created; everyone is allowed access.
Telnet	No	No policy is created; everyone is allowed access.
SNMP	No	No policy is created; everyone is allowed access.
Management Server	No	No policy is created; everyone is allowed access.
Serial Port	No	No policy is created; everyone is allowed access.
Front Panel	No	No policy is created; everyone is allowed access.

For more information on security level settings and how to apply them, see [“Creating a Secure Fabric”](#) on page 150.

When you click the security level radio buttons, the predefined policy settings are displayed in the table. You can change those settings by clicking in the check boxes for the policy and corresponding setting level (allow all, current Fabric/FM, allow none, and user-defined).

Creating a Secure Fabric

To launch the Create Secure Fabric wizard:

1. Click a fabric in the **SAN Elements** tab for which you want to enable secure mode.
2. Select **Actions > Security > Enable Secure Mode**.

Note: The **Actions > Security > Enable Secure Mode** option is applicable only to switches running future versions of Fabrics OS. If you have a switch or director running firmware version 4.2.x or earlier, these menu options are disabled. You should enable or disable secure mode using the CLI.

If login information is not set for any switch in the fabric, you are prompted to set the login information before continuing.

You cannot enable secure mode on a fabric unless all switches in the fabric have a Secure Fabric OS license, Zoning license, and security certificates installed. For more information about certificates, refer to the *HP StorageWorks Secure Fabric OS 4.2.x User Guide*.

The Create Secure Fabric wizard is launched (see [Figure 31](#)).

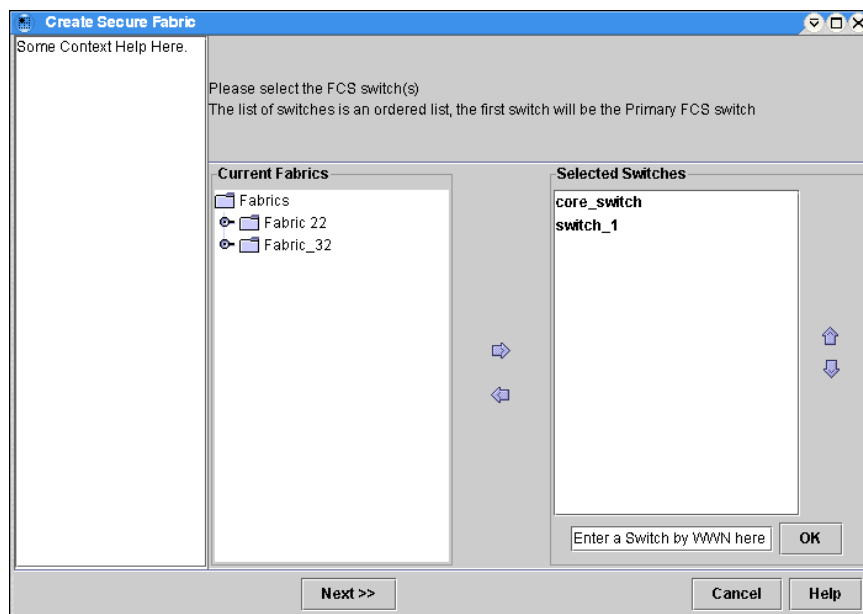


Figure 31: Select FCS Switches

3. Click **Name**, **IP address**, or **WWN** to select how the switches are displayed in the **Available Switches** list. Click the switches you want to be FCS switches from the **Available Switches** list.

If the switches you want to select are in another fabric, click the **Show All Fabrics** check box and then click the switches from the **Available Switches** list.

If the switches you want to select are not yet discovered, enter the switch WWN in the **Enter WWN** field under the FCS Switches panel, and click **OK**. The switch is added to the **FCS Switches** list.

4. Click the right arrow to move the selected switches to the **Selected Switches** list. The **Selected Switches** list is populated with the switches you selected. The first switch listed in the **FCS Switches** list is the Primary FCS switch.
5. Optional: Arrange the **FCS Switches** list order by using the up and down arrow buttons.
6. After the **FCS Switches** list is arranged in the correct order, click **Next**. The Create Passwords for Secure Fabric screen is displayed.
7. Do one of the following to set up your passwords:
 - Click **Keep Current Passwords** to keep all of your current passwords. Although this option is presented, it is not recommended. To ensure maximum security, it is best to reset your passwords. New passwords must be between 8 and 40 characters and must differ from the current passwords by at least one character.
 - Click **Use Same Passwords for all Accounts** and then enter a single password to use for all accounts. Although this option is presented, it is not recommended. To ensure maximum security, it is best to reset your passwords. New passwords must be between 8 and 40 characters and must differ from the current passwords by at least one character.
 - Enter new passwords for all user accounts and access levels. New passwords must be between 8 and 40 characters and must differ from the current passwords by at least one character.

Click **Next**.

8. Optional: You can create a set of policies as part of enabling secure mode (see [Figure 32](#)). The set of security policies is divided into 4 security levels: High, Medium, Low, and Custom. [Table 22](#), [Table 23](#), and [Table 24](#) explain which policies are created and who is allowed access for each security level.

Please select the security level for policy creation. Each level corresponds to a different policy set. To create custom policies, select the Custom radio button. Click the "Preview" button to preview the policies that will be created for a selected security level.

Select Security Policy Settings

Security Level: ☒ High ☐ Medium ☐ Low ☐ Custom

Policy Name	Allow All	Current Fabric/FM	Allow None	User-defined
SCC	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DCC	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
API	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
HTTP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Telnet	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
SNMP	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SES	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Management Se...	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Serial Port	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Front Panel	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Allow All: Any switch or device is allowed to connect in the fabric
 Current Fabric/FM: Fabric is locked down with only current switches/devices/FM allowed to connect
 Allow None: Access is denied from everywhere
 Custom: User defined policy set

<< Back Next >> Cancel Help

Figure 32: Select Security Policy Settings (Optional)

Click **Preview** to see exactly what policies are generated with the selected configurations. A new window is opened, displaying the policy settings that each security level generates. FCS and SCC policies are created by default even if you do not create a set of policies.

9. Click **Next**. A confirmation dialog box opens listing the new settings.
10. Review the new settings and then click **Finish** to exit the wizard.

Launching the Policy Editor

Log in to the Policy Editor to view and configure security policy options.

To launch the Policy Editor:

1. From the **SAN Elements** tab, click the primary FCS switch in the secure fabric for which you want to set policies.
2. Select **Actions > Security > Security Policy Editor**. The **Policy Editor** is displayed (see [Figure 30](#) on page 147).

Viewing and Configuring Security Policy Options

To configure security on a secure fabric:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **Summary** tab to view your defined policy sets and active policy sets.
3. To make changes to policies, click the **Policy** tab and do either of the following:
 - Make the changes and then click **Save** in the **Summary** tab to store your updates, but not activate them.
 - Click **Activate** in the **Summary** tab to activate the defined policy sets immediately. When you click **Save** or **Activate**, all policies are activated and saved.

Configuring FCS Policy Options

Switches in your FCS policy serve as *trusted switches*. The first switch in the policy serves as the primary FCS (from which you can configure your fabric), and each subsequent switch serves as a backup FCS. The order in which switches appear in the policy represents the order in which each backup switch takes over as primary FCS if the preceding primary FCS fails.

To edit the FCS policy:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **FCS** tab.

All switches in the selected fabric are displayed in the **Available Switches** list; the currently selected FCS switches are displayed in the **FCS Switches** list (see [Figure 33](#)).

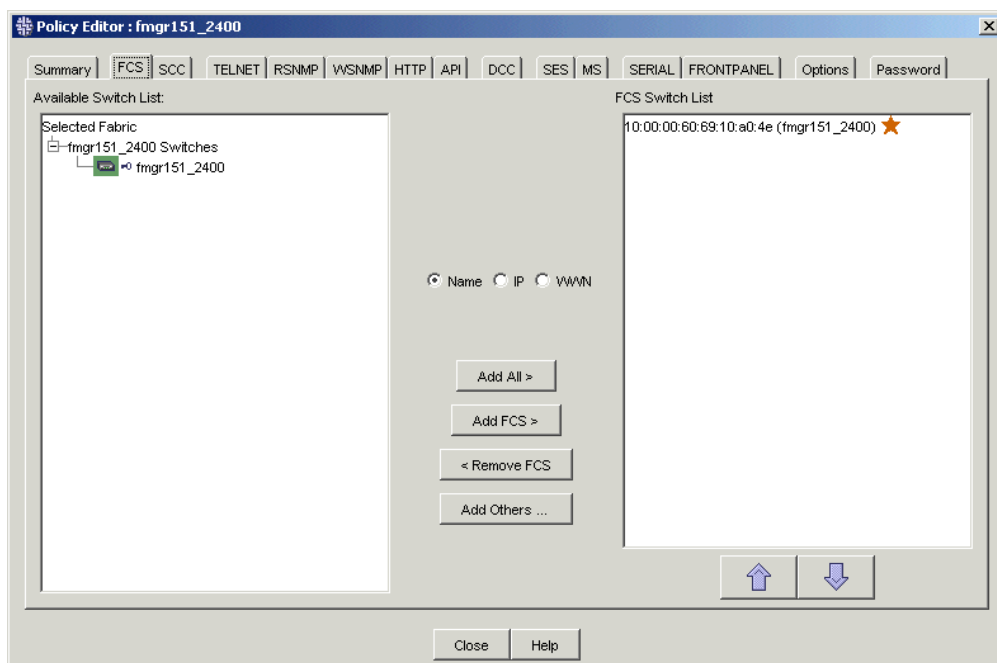


Figure 33: Configuring the FCS Policy

3. Click a switch from the **Available Switches** list and click **Add FCS** to add the switch to the **FCS Switches** list, or click **Add All** to all of the switches in the current fabric.

To add a switch WWN that is not included in the **Available Switches** list, click **Add Others** and then enter the WWN you want to add.

To remove a switch from the FCS policy, click the switch in the **Fabric Switches** list and then click **Remove FCS**.

The switches appear in the order in which they become a primary FCS switch if the primary FCS fails. You can rearrange the order of the switches using the up and down arrow keys. The primary FCS switch is marked with a **Star** icon next to it.

Note: Changing the Primary FCS causes updates in the fabric that might take time to complete, depending on the fabric size.

4. To save your changes or activate the policy with the changes, click the **Summary** tab.
5. Click **Save** (on the **Summary** tab) to save your changes, but not apply them, or click **Activate** (on the **Summary** tab) to save *and* apply your changes. When you click **Save** or **Activate**, all policies are activated and saved. The Security Policy Review dialog box opens.
6. After reviewing the security policy, click:
 - **Continue** to continue applying your changes.
 - **Cancel** to cancel your changes.
 - **Copy to File** to copy the Security Policy to a file.

Configuring SCC Policy Options

The SCC policy defines all switches in the secure fabric (FCS and non-FCS). You cannot add a new switch to a secure fabric without adding the switch to the SCC policy. You cannot add a switch to the SCC policy until you create an SCC policy. SCC policies are created automatically in Fabric Manager when you enable secure mode on a fabric.

To edit the SCC policy:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **SCC** tab. All current switches in the fabric are displayed in the **Available Switches** list ([Figure 34](#)).

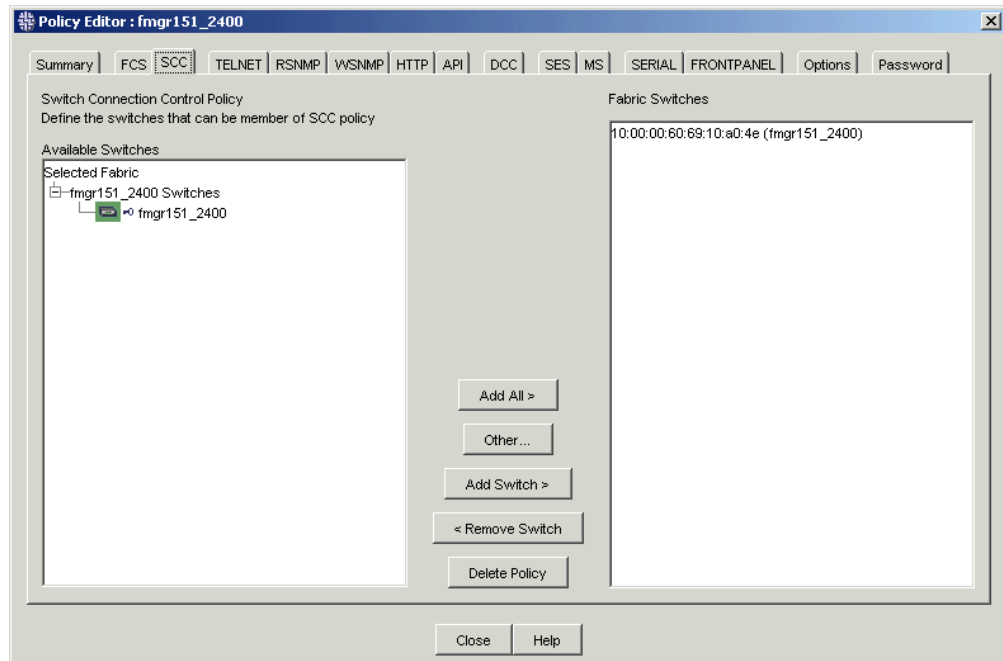


Figure 34: Configuring the SCC Policy

3. Click a switch that you want to include in that policy and then click **Add Switch**, or click **Add All** to add all switches from the fabric in that policy.

To add a switch WWN that is not listed in the **Available Switches** list, click **Other**, and enter the WWN you want to add.

Note: All switches within a fabric must be included in the SCC policy or else the excluded switches are segmented out into their own fabric.

4. To remove a switch from the SCC Policy, click the switch from the **Fabric Switches** list and then click **Remove Switch**.
5. To delete the policy, click **Delete Policy**.
6. To save your changes or activate the policy with the changes, click the **Summary** tab.
7. Click **Save** (on the **Summary** tab) to save your changes, but not apply them, or click **Activate** (on the **Summary** tab) to save *and* apply your changes. When you click **Save** or **Activate**, all policies are activated and saved.

Configuring Telnet, RSNMP, WSNMP, HTTP, and API Policy Options

The Telnet policy contains a list of IP addresses and subnets that can establish Telnet connections to any switch in the fabric. Telnet attempts fail from any IP address or subnet that does not appear in the policy. If you create an empty policy, you prevent all Telnet access to your fabric.

Configure the RSNMP policy (read-only SNMP policy) to limit SNMP access to specific, trusted management stations in your environment. You cannot create an RSNMP policy without a WSNMP policy already present.

Configure the WSNMP policy (read/write SNMP policy) to limit SNMP access to specific, trusted management stations in your environment. When you add a member to the WSNMP policy, that member automatically gains RSNMP access.

Configure the HTTP policy to grant access to IP addresses and subnets so they can establish HTTP connections to the switches in the fabric.

Create an API policy to control the workstations that can use the API to access the fabric.

To create any of these policies:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **Policy** tab, where *Policy* is **Telnet**, **RSNMP**, **WSNMP**, **HTTP**, or **API**. The Policy is displayed. [Figure 35](#) shows the **Telnet** policy tab as an example.

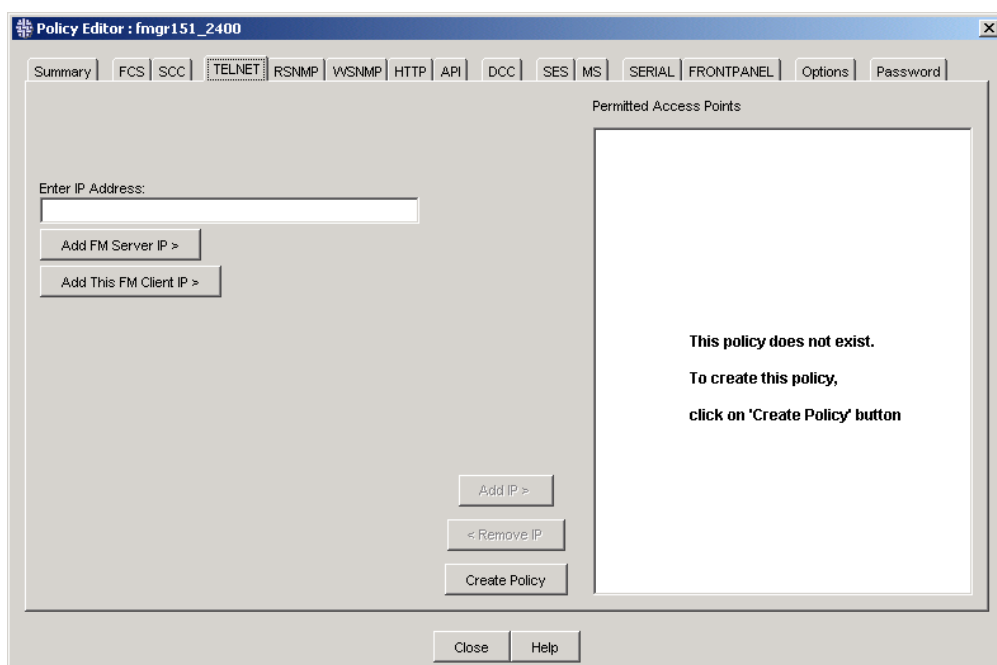


Figure 35: Configuring the Telnet Policy

3. Click **Create Policy**.

You have now created an empty policy, which denies the policy type (Telnet, RSNMP, WSNMP, HTTP, or API) access from all hosts to all switches in the fabric.



Caution: If you create either empty policies in the serial, Telnet, HTTP, and API policies simultaneously or policies without Fabric Manager Client/Server IP addresses, you can no longer manage security and you are no longer able to manage the switch.

If you use Fabric Manager to update the API policy to disable API access from the current host (either by creating an empty policy, or by specifically excluding this host from the **API Policy** list), the security transaction becomes locked and it can take up to two hours before Fabric OS releases the security transaction. You cannot modify the policies until the security transaction is released.

If you want to continue managing security and the switch, continue with the rest of the procedure.

4. Enter the IP address of a host that you want to include in the policy in the **Enter IP Address** field.
-

Note: The IP address of your Fabric Manager client must appear in the serial, Telnet, RSNMP, WSNMP, HTTP, and API policies or you cannot access the fabric with Fabric Manager.

5. Optional: Click **Add FM Server IP** to add the Fabric Manager server IP address, or click **Add this FM Client IP** to add the Fabric Manager client IP address.
6. Click **Add IP**. The IP address is displayed in the **Permitted Access Points** list.
7. To save your changes or activate the policy with the changes, click the **Summary** tab.
8. Click **Save** (on the **Summary** tab) to save your changes, but not apply them, or click **Activate** (on the **Summary** tab) to save *and* apply your changes. When you click **Save** or **Activate**, all policies are activated and saved. The Policy Review dialog box opens.
9. After reviewing the security policy, click one of the following:
 - **Continue** to continue applying your changes.
 - **Cancel** to cancel your changes.
 - **Copy to File** to save the policy to a file.

To make changes to your Telnet, RSNMP, WSNMP, HTTP, API or policy:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **Policy** tab, where *Policy* is **Telnet**, **RSNMP**, **WSNMP**, **HTTP**, or **API**.
3. Perform any of the following:
 - To remove a host from the **Permitted Access Points** field, click the IP address of a host in the field and then click **Remove IP**.
 - To delete the policy, click **Delete Policy**.

Configuring RSNMP Policy Options

Configure the read-only SNMP (RSNMP) policy to limit SNMP access to specific, trusted management stations in your environment. You cannot create a RSNMP policy without a WSNMP policy already present.

Note: You can launch the Security Admin only if the optional Security license is installed.

To create an RSNMP policy:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **RSNMP** tab.
3. Click **Create Policy**.
4. Enter the IP address of a host that you want to include in the policy in the **Enter IP Address** field.
5. Optional: Click **Add FM Server** to add the Fabric Manager server IP address, or click **Add FM Client** to add the Fabric Manager client IP address.
6. Click **Add IP**. The IP address is displayed in the **Permitted Access Points** field.
7. Click **Save** to save your changes, but not apply them, or click **Activate** to apply your changes.

To make changes to your RSNMP policy:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **RSNMP** tab.
3. Perform any of the following:
 - To remove a switch from the **Permitted Access Points** field, click the IP address of a switch in the field and click **Remove IP**.
 - To delete the RSNMP policy, click **Delete Policy**.

Configuring WSNMP Policy Options

Configure the WSNMP policy (read/write SNMP policy) to limit SNMP access to specific, trusted management stations in your environment. When you add a member to the WSNMP policy, that member automatically gains RSNMP access.

To create a WSNMP policy:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **WSNMP** tab.
3. Click **Create Policy**.
4. In the **Enter IP Address** field, enter the IP address of a host that you want to include in the policy.
5. Optional: Click **Add FM Server** to add the Fabric Manager server IP address, or click **Add FM Client** to add the Fabric Manager client IP address.
6. Click **Add IP**. The IP address is displayed in the **Permitted Access Points** field.

7. Click **Save** to save your changes, but not apply them, or click **Activate** to apply your changes.

To make changes to your WSNMP policy:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **WSNMP** tab.
3. Perform any of the following:
 - To remove a switch from the **Permitted Access Points** field, click the IP address of a switch in the field and click **Remove IP**.
 - To delete the WSNMP policy, click **Delete Policy**.

Configuring HTTP Policy Options

Configure the HTTP policy to grant access to IP addresses and subnets, so they can establish HTTP connections to the switches in the fabric.

Note: The IP address of your Fabric Manager client must appear in this policy or you cannot access the fabric with Fabric Manager.

To create an HTTP policy:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **HTTP** tab.
3. Click **Create Policy**. You have now created an empty policy, which denies serial access to all switches in the fabric.



Caution: If you create either empty policies in the serial, Telnet, HTTP, and API policies simultaneously or policies without Fabric Manager Client/Server IP addresses, you can no longer manage security and you are not able to manage the switch. If you want to continue to manage security and the switch, continue with the rest of the procedure.

4. In the **Enter IP Address** field, enter the IP address of a host that you want to include in the policy.
5. Optional: Click **Add FM Server** to add the Fabric Manager server IP address, or click **Add FM Client** to add the Fabric Manager client IP address.
6. Click **Add IP**. The IP address is displayed in the **Permitted Access Points** field.
7. Click **Save** to save your changes, but not apply them, or click **Activate** to apply your changes.

To make changes to your HTTP policy:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **HTTP** tab.

3. Perform any of the following:
 - To remove a switch from the **Permitted Access Points** field, click the IP address of a switch in the field and then click **Remove IP**.
 - To delete the HTTP policy, click **Delete Policy**.

Configuring API Policy Options

Create an API policy to control the workstations that can use the API to access the fabric.



Caution: If you use Fabric Manager to update the API policy, to disable API access from the current host (either by creating an empty policy or by excluding this host from the **API Policy** list), the security transaction becomes locked and it can take up to two hours before Fabric OS releases the security transaction. You cannot modify the policies until the security transaction is released.

To create a API policy:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **API** tab.
3. Click **Create Policy**. You have now created an empty policy, which denies serial access to all switches in the fabric.



Caution: If you create either empty policies in the serial, Telnet, HTTP, and API policies simultaneously or policies without Fabric Manager Client/Server IP addresses, you can no longer manage security and are no longer be able to manage the switch. If you want to continue managing security and the switch, continue with the rest of the procedure.

4. In the **Enter IP Address** field, enter the IP address of a switch that you want to include in the policy.
5. Optional: Click **Add FM Server** to add the Fabric Manager server IP address or click **Add FM Client** to add the Fabric Manager client IP address.
6. Click **Add IP**. The IP address is displayed in the **Permitted Access Points** field.
7. Click **Save** to save your changes, but not apply them, or click **Activate** to apply your changes.

To make changes to your API policy:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **API** tab.
3. Perform any of the following:
 - To remove a switch from the **Permitted Access Points** field, click the IP address of a switch in the field and click **Remove IP**.
 - To delete the API policy, click **Delete Policy**.

Configuring DCC Policy Options

Configure DCC policies to bind device ports to specific switch ports. With Fabric Manager, you can create and configure multiple DCC policies with unique names. Populate DCC policies with switch and device WWNs.

To create a DCC policy:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **DCC** tab (see [Figure 36](#)).

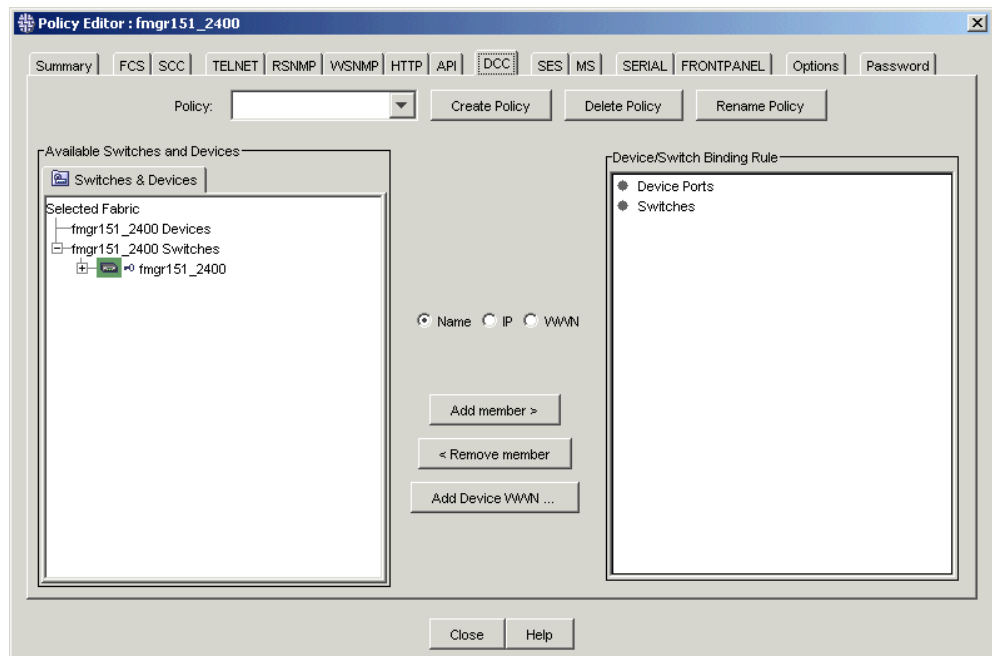


Figure 36: Configuring the DCC Policy

3. Click **Create Policy**. The Enter DCC Policy dialog box opens.
4. Enter a name for the new policy in the **Enter Policy Name** field and click **Create** in the Enter DCC Policy dialog box. The name is displayed in the **Policy** menu in the **DCC** tab.
5. Optional: Click **Name**, **IP**, or **WWN** to change how the switches and devices are displayed in the **Available Switches and Devices** list.

6. Click a switch or device WWN from the **Switches and Devices** tab to add to the policy and then click **Add Member**.

To add a WWN that is not displayed, click **Add Device WWN** and enter the WWN you want to add.

7. To save your changes or activate the policy with the changes, click the **Summary** tab.
8. Click **Save** (on the **Summary** tab) to save your changes, but not apply them, or click **Activate** (on the **Summary** tab) to save *and* apply your changes. When you click **Save** or **Activate**, all policies are activated and saved. The Policy Review dialog box opens.
9. After reviewing the security policy, click one of the following:
 - **Continue** to continue applying your changes.
 - **Cancel** to cancel your changes.
 - **Copy to File** to copy the policy to a file.

To make changes to your DCC policies:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **DCC** tab.
3. Perform any of the following actions for each individual DCC policy:
 - To remove a DCC policy, select **Policy > Policy Name You want to delete** and click **Delete Policy**.
 - To rename a DCC policy, select **Policy > Policy Name You want to rename** and click **Rename Policy**.
 - To change the contents of a DCC policy, select **Policy > Policy Name you want to edit**.
 - Click a switch or device WWN from the **Switches and Devices** tab to add to the policy and then click **Add Member**.
 - To add a WWN that is not displayed, click **Add Device WWN** and enter the WWN you want to add.
 - Click **Save** to save your changes, but not apply them, or click **Activate** to apply your changes.

Configuring MS Policy Options

Create an MS policy to allow trusted fabric-connected devices to access the management server. With Fabric Manager, you can create and configure multiple MS policies with unique names. Populate MS policies with switch and device WWNs. MS and MS policies are device-based. To create an MS policy:

Note: You can launch the Security Admin only if the optional Security license is installed.

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **MS** tab.
3. Click **Create Policy**. The WWN of a device that connects to the fabric is displayed in the **Permitted Access Points** field.
4. Click a device from the **Permitted Access Points** field.
5. Click **Add Device**.
6. Click **Save** to save your changes, but not apply them, or click **Activate** to apply your changes.

To make changes to your MS policy:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **MS** tab.

3. Perform any of the following:
 - To delete the policy, click the **Delete Policy** button.
 - To add a device to the policy, click the device in the **Available Access Points** field and then select the **Add Device > button** (click the **Save** or **Activate** button as appropriate.)
 - To remove a device from the policy, click the device in the **Permitted Access Points** field and then select the **Remove Device > button** (click the **Save** or **Activate** button as appropriate.)

Configuring Serial and Front Panel Policy Options

Create a serial policy to grant serial port access to specific switches.



Caution: If you create either empty policies in the serial, Telnet, HTTP, and API policies simultaneously or policies without Fabric Manager Client/Server IP addresses, you can no longer manage security and you are no longer able to manage the switch.

To create a serial or front panel policy:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **Policy** tab, where *Policy* is **Serial** or **Front Panel**. [Figure 37](#) shows the **Serial** tab.

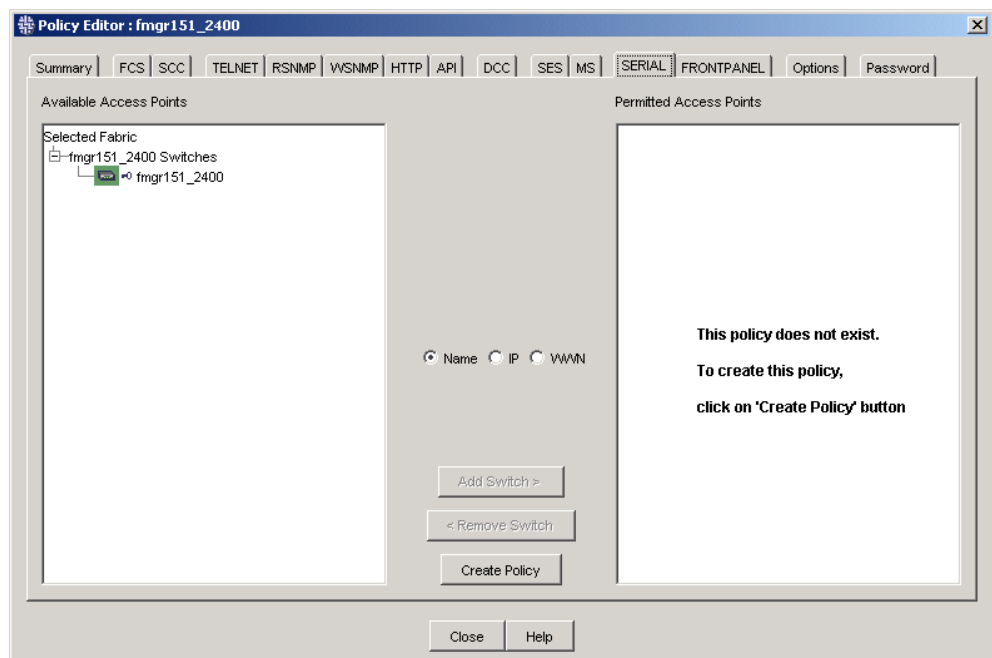


Figure 37: Configuring the Serial Policy

3. Click **Create Policy**. You have now created an empty policy, which denies serial and front panel access from all hosts to all switches in the fabric.



Caution: If you create either empty policies in the serial, Telnet, HTTP, and API policies simultaneously or policies without Fabric Manager Client/Server IP addresses, you can no longer manage security and you are no longer able to manage the switch.

If you want to continue managing security and the switch, continue with the rest of the procedure.

4. Optional: Click **Name**, **IP**, or **WWN** to change how the switches and devices are displayed in the **Available Access Points** list.
5. Click a switch in the **Available Access Points** field and click **Add Switch** to add it to your policy. Repeat this step for each switch that you want to add.
6. To save your changes or activate the policy with the changes, click the **Summary** tab.
7. Click **Save** (on the **Summary** tab) to save your changes, but not apply them, or click **Activate** (on the **Summary** tab) to save *and* apply your changes. When you click **Save** or **Activate**, all policies are activated and saved. The Policy Review dialog box opens.
8. After reviewing the security policy, click:
 - **Continue** to continue applying your changes.
 - **Cancel** to cancel your changes.
 - **Copy to File** to copy the policy to a file.

To make changes to your serial or front panel policy:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **Serial** tab.
3. Perform any of the following:
 - To add a switch to the policy, click the switch in the **Available Access Points** field and then click **Add Switch**. (Click the **Save** or **Activate** button as appropriate.)
 - To remove a host from the policy, click the host in the **Permitted Access Points** field and then click **Remove Switch**. (Click the **Save** or **Activate** button as appropriate.)

Configuring Front Panel Policy Options

Configure the front panel policy to enable front panel access to specific switches. To create a front panel policy, perform the following steps:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **Front Panel** tab.
3. Click **Create Policy**. You have now created an empty policy, which denies front panel access to all switches in the fabric. If you do not want to deny front panel access to all switches in the fabric, complete the steps in this procedure to add members to the policy.
4. Click a switch in the **Available Access Points** field and click **Add Switch** to add it to your policy. Repeat this step for each switch that you want to add.
5. Click **Save** to save your changes, but not apply them, or click **Activate** to apply your changes.

To make changes to your front panel policy:

1. Launch the Security Admin, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **Front Panel** tab.
3. Perform any of the following:
 - To delete the policy, click **Delete Policy**.
 - To add a switch to the policy, click the switch in the **Available Access Points** field and then click **Add Switch**. (Click the **Save** or **Activate** button as appropriate.)
 - To remove a switch from the policy, click the switch in the **Permitted Access Points** field and then click **Remove Switch**. (Click the **Save** or **Activate** button as appropriate.)

Configuring No Node WWN Zoning

Fabric Manager allows you to enable or disable no-node WWN zoning. When you enable this feature, security becomes port-oriented. Devices have port and node WWNs. When you disable node zoning, you ensure that devices with multiple ports cannot access secure fabrics with node WWNs. You must add individual port WWNs to your policies for devices to access your secure fabric.

To configure no-node WWN zoning:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **Options** tab.
3. To enable no-node WWN zoning, check the **No Node WWN Zoning** check box; to disable, uncheck the **No Node WWN Zoning** check box.
4. Click **Save** (on the **Summary** tab) to save your changes, but not apply them, or click **Activate** (on the **Summary** tab) to save *and* apply your changes. When you click **Save** or **Activate**, all policies are activated and saved.

Changing the FCS or Non-FCS Admin Security Password

To change the password that implements security, perform the following steps:

1. Launch the Policy Editor, as described in “[Launching the Policy Editor](#)” on page 152.
2. Click the **Password** tab (see [Figure 38](#)).

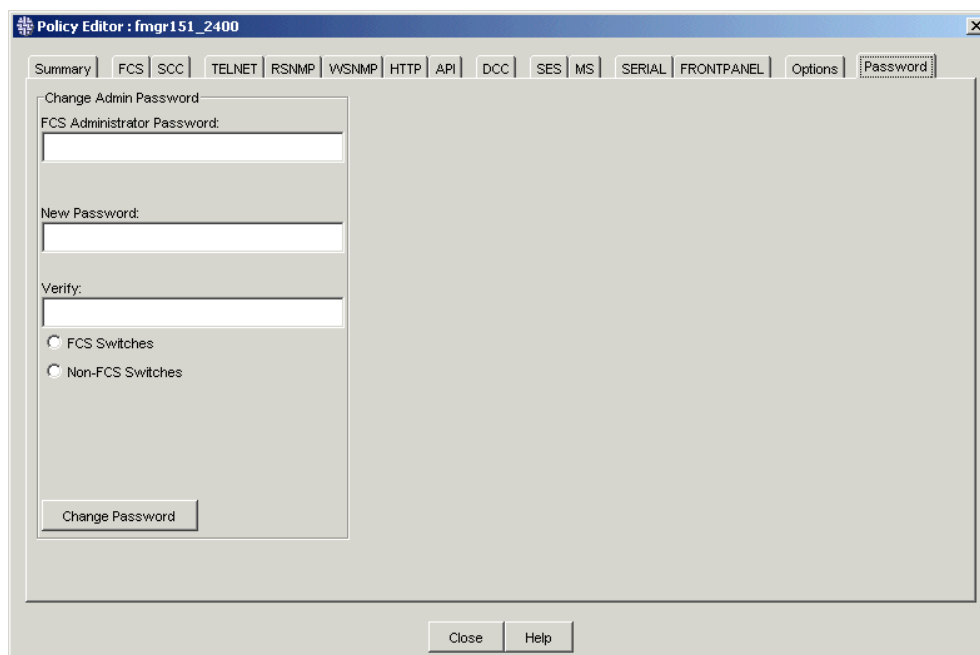


Figure 38: Configuring the FCS or Non-FCS Admin Security Password

3. Enter the current password in the **FCS Administrator Password** field.
4. Enter the new password in the **New Password** field. Passwords must be between 8 and 40 characters and must differ from the old password by at least one character.
5. Enter the new password again in the **Verify** field.
6. Click **FCS Switches** to change the admin password for Secure FCS switches only or click **Non-FCS Switches** to change the admin password for Secure Non-FCS switches only.
7. Click **Change Password**.
8. Click **Save** (on the **Summary** tab) to save your changes, but not apply them, or click **Activate** (on the **Summary** tab) to save *and* apply your changes. When you click **Save** or **Activate**, all policies are activated and saved.

Telnet on a Secure Fabric

The Telnet-to-FCS option is accessible for a secure fabric only when that fabric is selected in the **SAN Elements** tab; when a nonsecure fabric is selected, only the default Telnet option is accessible from the **Actions** menu.

SecTelnet is launched instead of the default Telnet client for fabrics running a secure firmware version.

Opening a Telnet Session for a Secure Fabric

To open a Telnet session for a secure fabric:

1. Click a secure fabric from the **SAN Elements** tab.
2. Select **File > Telnet to FCS**. The SecTelnet prompt is displayed. You can also open a Telnet session by right-clicking a switch from the **SAN Elements** tab.
3. Log in with your login ID and password.

Note: If a SecTelnet session is already active on a secure switch running firmware versions 2.6.x or 3.1.0 and you attempt to launch a new session, you receive the message, *Sorry, this system is engaged*. You must close the open Telnet session and relaunch Telnet for the secure switch.

Merging Secure Fabrics

To merge secure fabrics that are not physically connected to each other into one fabric:

1. From the **SAN Elements** tab, click a secure fabric that you want to merge into a primary secure fabric. This fabric is to be the secondary fabric.
2. Select **Actions > Security > Merge with Secure Fabric**. The Merge Secure Fabrics wizard launches.
3. Click the primary fabric that you want to merge the other fabric into and then click the right arrow to move it over.
4. Click **Next**.
5. Click switches that you want to be the FCS switches for the merged fabric.
6. Click the right arrows to move them over.
7. Select the **Security Policy Settings**.
8. Click **Next**. A confirmation dialog box displays the selected settings for the new merged fabric.
9. After reading the confirmation, click **Finish** to exit the wizard. You can now physically connect the two fabrics.

Adding a Switch to a Secure Fabric

If you attempt to add a new switch to a secure fabric the same way you would add it to a non-secure fabric, the switch is rejected and segmented into its own fabric. To add the switch successfully, secure mode must first be enabled on the switch and you must define the **FCS** list for the switch. The **FCS** list must also be exactly the same as the **FCS** list of the secure fabric. For instructions on adding a switch to the SCC policy, see “[Configuring SCC Policy Options](#)” on page 154.

To add a switch to a secure fabric:

1. Enable secure mode on a single switch in a nonsecure fabric (see “[Creating a Secure Fabric](#)” on page 150),
2. Merge the secure fabrics into one fabric using the secure fabric wizard (see “[Merging Secure Fabrics](#)” on page 166).

Using the Zoning Module in Fabric Manager

21

Fabric Manager uses Advanced Web Tools to configure and administer zoning. When you select zone edit in Fabric Manager, it launches zone edit from Advanced Web Tools. This chapter provides Advanced Web Tools instructions for switches running firmware version 4.2.x. If you have switches running other versions of firmware, refer to the Advanced Web Tools documentation supporting the appropriate version of firmware.

Note: A zoning license and administrative privileges are required to access the Zone Admin module. Specific Advanced Web Tools interfaces vary by firmware. Your interface and functionality may not match the interface that is shown in the figures and examples in this chapter.

Zoning enables you to partition your SAN into logical groupings of devices that can access each other. For example, you can partition your SAN into two zones, *winzone* and *unixzone*, so that your Windows servers and storage do not interact with your UNIX servers and storage. To configure zoning, you must use zones, aliases, and configurations.

If you plan to add a switch to a fabric that uses zoning, discover that switch with Fabric Manager and run a merge check between that switch and the fabric to which you plan to add it. This check identifies any zoning and configuration mismatches before you physically connect the switch.

Zone

A *zone* is a region within the fabric where switches and devices can communicate. A device can communicate only with other devices connected to the fabric within its specified zone. You can specify members of a zone based on the following identifiers:

- Alias names
- Switch domain and port area number pairs (for example, 2 , 20)
- WWNs
- QuickLoop AL_PAs

Note: QuickLoop is not a supported features for switches running 4.x firmware versions. Switches running Fabric OS v4.x cannot be part of a QuickLoop. The 4.x versions of firmware do not support the QuickLoop feature. Switches running 2.x or 3.x versions of firmware that are in the same fabric as a launch switch running 4.x are displayed as QuickLoop members.

Alias

An *alias* is a logical group of ports, WWNs, or AL_PAs. Specifying groups of ports or devices as an alias makes zone configuration easier by enabling you to configure zones using an alias rather than a long string of individual members. You can specify members of an alias using the following methods:

- A switch domain and port area number pair; for example, 2 , 20.
- WWN (device)
- QuickLoop AL_PAs (device)

Configuration

A *configuration* (often called a *config*) is a group of zones. Zoning is enabled on a fabric by enabling a specific configuration. You can specify members of a configuration with the following identifiers:

- Zone names
- QuickLoop names
- Fabric Assist (FA) zone names

Zoning Schemes

Various levels of zoning (or *zoning schemes*) isolate systems that have different operating environments. For example, you can create a zone of all ports connected to UNIX servers, or another zone of all ports connected to Windows servers. Zones limit access of devices to other devices connected to the fabric within the same zone.

Zones can be configured dynamically. They can vary in size depending on the number of fabric connected devices, and devices can belong to more than one zone. Because zone members can access only other members of the same zone, a device not included in a zone is not available to members of that zone.

Security

When you enable security, you can access zoning only with the primary FCS switch. The zoning icon does not appear on any other switch in the display. If you do not enable security, you can configure zoning from any switch.

Zoning Methods

Zoning methods determine what is displayed in the subsequent components of the Zone Administration window. You can use four methods to define members of a zone. Each method is considered either hard zoning or soft zoning. Hard zoning defines alias members exclusively with domain/port ID pairs or with WWNs. Soft zoning defines alias members with a mixture of port IDs and WWNs. [Table 25](#) describes the methods.

Table 25: Zoning Methods

Method	Description
Mixed Zoning	This method enables you to define members using the port area number, device WWNs, QuickLoop AL_PAs. This method is considered soft zoning.
Port Zoning	This method enables you to define members using port area number only. This method is considered hard zoning.
WWN Zoning	This method enables you to define members of zone using device WWNs. This method is considered hard zoning.
AL_PA Zoning	This method enables you to define members of zone using QuickLoop AL_PAs only. This method is considered hard zoning.

Zoning Method and Tabs Available

Depending on the zone method that you use, certain tabs may or may not be available on the Zone Administration window (see [Table 26](#)).

Table 26: Zone Methods and Tabs Table

Zone Level	Available Tabs
Mixed Zoning	Alias, Zone, QuickLoop, Fabric Assist, Config
Port Zoning	Alias, Zone, QuickLoop, Fabric Assist, Config
WWN Zoning	Alias, Zone, QuickLoop, Fabric Assist, Config
AL_PA Zoning	Alias, Zone, QuickLoop, Config

Accessing the Zone Administration Module

To access the Zone Administration module:

1. Click the fabric you want to view from the **SAN Elements** tab.
2. Select **Actions > Zone Admin**. Advanced Web Tools launches and prompts you to log in to the Zone Administration module.
3. Enter the admin user name and password. The Zone Administration module is displayed.

Creating a Zone Configuration

A configuration is a group of zones; zoning is enabled on a fabric by enabling a specific configuration. You can specify members of a configuration using the following methods:

- Zone names
- QuickLoop names
- FA (Fabric Assist) zone names

Sample Configuration

Table 27 shows a sample zoning configuration.

Table 27: Sample Zoning Database

Alias	Zone	Config
alias1 = WWN; WWN; WWN		
alias2 = WWN; <domain, portarea>		
alias3 = WWN; <AL_PA>	zone1 = alias1; alias2; WWN; <domain, portarea>; <ALPA>	
alias4 = WWN; WWN; WWN	zone2 = alias3, alias4, WWN	myconfig = zone1, zone2

To create a zone configuration:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Optional: If you want to stay with mixed zoning (default), skip this step. Otherwise, select one of the following methods to view members from the **View** menu:
 - Mixed zoning
 - Port zoning
 - WWN zoning
 - AL_PA zoning

The member view method you choose determines how members are displayed in the **Member Selection** list. See “[Selecting a Zoning Method](#)” on page 172 for more information.
3. Click the **Config** tab.
4. Click **Create**. The Create New Config dialog box opens.
5. Enter a name for the new configuration and click **OK**.
6. Click + signs in the **Member Selection** list to view the nested elements. The choices available in the **Member Selection** list depend on the selection made in the **View** menu.
7. Highlight an element in the **Member Selection** list that you want to include in your configuration. The **Add Member** button becomes active.
8. Click **Add Member** to add configuration members. Selected members are moved to the Config Members window.
9. Repeat [step 7](#) and [step 8](#) to add more elements to your configuration.
10. Select **Actions > Save Config Only**. The new configuration is displayed in the **Name** list. To enable the configuration, see “[Enabling a Zone Configuration](#)” on page 173.

Note: Changes made to the currently enabled configuration do not appear until the configuration is reenabled.

Displaying the Enabled Zone Configuration

To view the enabled zone configuration:

Select the desired switch from the Fabric tree.

The selected switch is displayed in the [Switches View](#). The current zone configuration (if one is enabled) is displayed in the lower portion of the Switch Information View. If no zone configuration is enabled, the field displays none.

Displaying the Zone Configuration Summary

To view a zone configuration summary report:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **File > Print Summary**. The Zone Configuration Summary dialog box opens.

Note: The summary displays the information based on the changes just made. If the changes were not committed correctly, the Zone Configuration Summary might not match the actual zone configuration settings.

Adding a WWN to the Zoning Database

To add a WWN to the zoning database:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **Edit > Add a WWN**. The Add WWN dialog box opens.
3. Enter a WWN value in the **WWN** field.
4. Click **OK**. The Add WWN dialog box opens. It lists all the zoning elements for the new WWN, including aliases, zones, and FA zones.
5. Click an item in the list to select or unselect and then click **Add** to add the new WWN to all the selected zoning elements. The WWN is added to the zoning database and can be used as a member.

Note: The added WWN does not need to currently exist in the Fabric. This procedure enables you to configure a WWN as a member in a zone configuration before adding that device to the fabric. It is especially useful if you want to add a WWN to all or most zoning entities.

Deleting a WWN from the Zoning Database

To delete a WWN from the zoning database:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **Edit > Delete a WWN**. The Delete WWN dialog box opens.
3. Enter a WWN value in the **WWN** field.

4. Click **OK**. The Delete WWN dialog box opens. It lists all the zoning elements that include the WWN.
5. Click an item in the list to select or unselect and then click **Delete** to delete the WWN from all the selected zoning elements. The WWN is deleted from the zoning database.

Replacing a WWN in the Zoning Database

This procedure enables you to replace a WWN throughout the zoning database. This is useful when exchanging devices in your fabric and helps you to easily maintain your current configuration.

To replace a WWN in the zoning database:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **Edit > Replace a WWN**. The Replace WWN dialog box opens.
3. Enter the WWN to be replaced in the **Replace** field.
4. Enter the new WWN in the **By** field.
5. Click **OK**. The Replace WWN dialog box opens. It lists all the zoning elements that include the WWN.
6. Click an item in the list to select or unselect and then click **Replace** to replace the WWN in all the selected zoning elements. The old WWN is replaced in the zoning database by the new WWN, including within any alias or zone of which the old WWN was a member.

Searching for a Zone Member

You can search zone members for specified strings of text. To search for a zone member:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **Edit > Search Member**.
3. Enter the zone member name in the **Member Name** field. You can narrow the search by checking one or more of the check boxes, such as **Match Case**.
4. Click **Next** to begin the zone member search.

Selecting a Zoning Method

The zoning method you choose determines how members are displayed in the various member selection windows. There are four methods of defining members for zoning described in [Table 25](#) on page 169.

For more specific information about zoning, or for information about configuring zones using the Fabric OS command-line *interface (CLI)*, refer to the *HP StorageWorks Fabric OS 4.2.x Features User Guide* and the *HP StorageWorks XPath OS Version 7.1.x Procedures User Guide*.

The zoning method you choose determines what is displayed in subsequent Zone Administration windows. The zoning method you choose is displayed in the header of the Zone Administration window. Depending on the method you choose, certain tabs might or might not be available on the Zone Administration window.

For more detailed information about zoning, refer to the *HP StorageWorks Fabric OS 4.2.x Features User Guide*.

To select a zoning method:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. From the **View** menu, select one of the following:
 - Mixed Zoning
 - Port Zoning
 - WWN Zoning
 - AL_PA Zoning

Refreshing the Fabric

To refresh the fabric:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **View > Refresh Fabric**. This refreshes the status for the fabric, including switches, ports, and devices.

Enabling a Zone Configuration

Select **Actions > Enable a Config** to enable a configuration that has previously been created (see “[Creating a Zone Configuration](#)” on page 169). After the dialog box opens, select the desired configuration from the menu.

Several configurations can reside on a switch at once and you can quickly alternate between them. For instance, you might want to have one configuration enabled during business hours and another enabled overnight. Only one zone configuration can be enabled at a time. To create a new configuration, see “[Creating a Zone Configuration](#)” on page 169.

To enable a zone configuration:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **Actions > Enable Config**. The Enable Config dialog box opens.
3. Select the configuration to be enabled from the menu. A warning is displayed.
4. Click **Yes** to save and enable the selected configuration.

Disabling a Zoning Configuration

When you disable the active configuration, the zoning feature is disabled on the fabric and all devices within the fabric can communicate with all other devices. This does not mean that the zoning database is deleted; it means that there is no configuration active on the fabric.

To disable a zoning configuration:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **Actions > Disable Zoning**. The Disable Config warning is displayed.
3. Click **Yes** to save and disable the current configuration.

Saving Changes to an Existing Configuration

To save a configuration:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Config** tab.
3. Make desired changes to the configuration (see “[Creating a Zone](#)” on page 177). You can make changes only to a configuration that is currently enabled; changes do not appear, however, until the configuration is disabled and re-enabled.
4. Select **Actions > Save Config Only**. To enable the configuration, see “[Enabling a Zone Configuration](#)” on page 173.

Refreshing the Zoning Database

To refresh the zoning database:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **View > Refresh Zoning**.

This refreshes the zoning database and the fabric. Any unsaved zoning changes are deleted. The current zoning database can be viewed from the Zone Configuration Summary screen. See “[Displaying the Zone Configuration Summary](#)” on page 171 for more information.

Clearing the Zoning Database

To disable any active configuration and delete the entire zoning database:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **Actions > Clear All**. The Disable Config warning is displayed.



Caution: This action not only disables zoning on the fabric, but deletes the entire zoning database, which results in all devices being able to communicate with all other devices.

3. Click **Yes** to disable the current configuration.

Creating a Zone Alias

An alias is a logical group of ports, WWNs, or AL_PAs. Specifying groups of ports or devices as an alias makes zone configuration easier by enabling you to configure zones using an alias rather than a long string of individual members. You can specify members of an alias using the following methods:

- A switch domain and port area number pair: for example, 2 , 20.
- WWN (device)
- QuickLoop AL_PAs (device)

To create an alias:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select one of the following methods to view members from the **View** menu:
 - Mixed zoning
 - Port zoning
 - WWN zoning
 - AL_PA zoning

The member view method you choose determines how members are displayed in the **Member Selection** list.

3. Click the **Alias** tab.
4. Click **Create Alias**. The Create New Alias dialog box opens.
5. Enter a name for the new alias.
6. Click **OK**.
7. Click + signs in the **Member Selection** list to view the nested elements. The choices available in the **Member Selection** list depend on the selection made in the **View** menu.
8. Click an element in the **Member Selection** list that you want to include in your alias. The **Add Member** button becomes active.
9. Click **Add Member** to add alias members. Selected members are moved to the Alias Members window.

10. Repeat [step 8](#) and [step 9](#) to add more elements to your alias.
11. Optional: Click **Add Other** to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric. The new alias is displayed in the **Name** list.

Modifying the Members of a Zone Alias

To modify the members of an alias:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Alias** tab.
3. Select the alias you want to modify from the **Name** menu.
4. Highlight an element in the **Member Selection** list that you want to include in your alias or highlight an element in the **Alias Members** list that you want to delete.
5. Click **Add Member** to add an alias member or click **Remove Member** to remove an alias member.

Deleting a Zone Alias

Perform the following procedure to remove a zone alias from the zoning database. After a zone alias is deleted, it is longer a member of the zones it was once a member of.

To delete an alias:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Alias** tab.
3. From the **Name** menu, select the alias you want to delete.
4. Click **Delete**. The Confirm Deleting Alias screen is displayed.
5. Click **OK**. The selected alias is deleted from the zoning database.

Renaming a Zone Alias

To rename an alias:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Alias** tab.
3. From the **Name** menu, select the alias you want to rename.
4. Click **Rename**. The Rename an Alias dialog box opens.
5. Enter a new alias name and click **OK**. The alias is renamed in the zoning database.

Creating a Zone

A zone is a region within the fabric in which specified switches and devices can communicate. A device can communicate only with other devices connected to the fabric within its specified zone.

To create a zone, perform the following steps:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select one of the following methods to view members from the **View** menu:

- Mixed zoning
- Port zoning
- WWN zoning
- AL_PA zoning

The member view method you choose determines how members are displayed in the **Member Selection** list. See “[Accessing the Zone Administration Module](#)” on page 169 for more information.

3. Click the **Zone** tab.
4. Click **Create**. The Create New Zone dialog box opens.
5. Enter a name for the new zone in the Create New Zone dialog box and then click **OK**.
6. Click + signs in the **Member Selection** list to view the nested elements. The choices available in the **Member Selection** list depend on the selection made in the **View** menu.
7. Select an element in the **Member Selection** list that you want to include in your zone. The **Add Member** button becomes active.
8. Click **Add Member** to add the zone member. The selected member is moved to the Zone Members window.
9. Repeat [step 7](#) and [step 8](#) to add more elements to your zone.
10. Click **Add Other** to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric (optional). The new zone is displayed in the **Name** list.

Modifying the Members of a Zone

To modify the members of a zone:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Zone** tab.
3. Click the zone you want to modify from the **Name** menu. The zone members for the selected zone are listed in the **Zone Members** list.
4. Click an element in the **Member Selection** list that you want to include in your zone or click an element in the **Zone Members** list that you want to delete.
5. Click **Add Member** to add a zone member.
6. Click **Remove Member** to remove a zone member.

Deleting a Zone

To delete a zone:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Zone** tab.
3. From the **Name** menu, click the zone you want to delete.
4. Click **Delete**. The Confirm Deleting Zone dialog box opens.
5. Click **OK**. The selected zone is deleted from the zoning database.

Renaming a Zone

To rename a zone:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Zone** tab.
3. Select the zone you want to rename from the **Name** menu.
4. Click **Rename**. The Rename a Zone dialog box opens.
5. Enter a new zone name and click **OK**. The zone is renamed in the zoning database.

Creating a QuickLoop

Note: You must have a QuickLoop license installed to create or modify a QuickLoop.

QuickLoop is an HP StorageWorks software product that allows multiple ports on a switch to create a logical loop. Devices connected via QuickLoop appear to each other as if they are on the same arbitrated loop.

QuickLoop can be administered using Fabric OS v4.x versions. Switches or directors running Fabric OS v4.x, however, cannot be members of a QuickLoop.

To create a QuickLoop:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select one of the following methods to view members from the **View** menu:
 - Mixed zoning
 - Port zoning
 - WWN zoning
 - AL_PA zoning

The member view method you choose determines how members are displayed in the **Member Selection** list. See “[Accessing the Zone Administration Module](#)” on page 169 for more information.

3. Click the **QuickLoop** tab.

4. Click **Create**. The Create New QuickLoop dialog box opens.
5. Enter a name for the new QuickLoop.
6. Click **OK**.
7. Click + signs in the **Member Selection** list to view the nested elements. The choices available in the **Member Selection** list depend on the selection made in the **View** menu.
8. Click an element in the **Member Selection** list that you want to include in your QuickLoop. The **Add Member** button becomes active.

Note: A QuickLoop may contain no more than two members. Only switches capable of running QuickLoop are displayed in the **Member Selection** list.

9. Click **Add Member** to add QuickLoop members. Selected members are moved to the **QuickLoop Members** area.
10. Repeat [step 8](#) and [step 9](#) to add more elements to your QuickLoop.
11. Optional: Click **Add Other** to include a WWN, port, or QuickLoop (AL_PA) that is not currently a part of the fabric. The new QuickLoop is displayed in the **Name** list.

Modifying QuickLoop Members

QuickLoop can be administered using Fabric OS v4.2.x. Switches running Fabric OS v4.x, however, cannot be members of a QuickLoop.

To modify the members of a QuickLoop:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **QuickLoop** tab.
3. From the **Name** menu, click the QuickLoop you want to modify.
4. Click an element in the **Member Selection** list that you want to include in your QuickLoop or click an element in the **QuickLoop Members** that you want to delete.
5. Click **Add Member** to add a QuickLoop member.
6. Click **Remove Member** to remove a QuickLoop member.

Deleting a QuickLoop

QuickLoop can be administered using Fabric OS v4.2.x. Switches running Fabric OS v4.x, however, cannot be members of a QuickLoop.

To delete a QuickLoop:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **QuickLoop** tab.
3. From the **Name** menu, click the QuickLoop you want to delete.
4. Click **Delete**. The Confirm Deleting QuickLoop dialog box opens.
5. Click **OK**. The selected QuickLoop is deleted from the zoning database.

Renaming a QuickLoop

QuickLoop can be administered using Fabric OS v4.2.x. Switches running Fabric OS v4.x, however, cannot be members of a QuickLoop.

To rename a QuickLoop:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **QuickLoop** tab.
3. From the **Name** menu, click the QuickLoop you want to delete.
4. Click **Rename**. The Rename a QuickLoop dialog box opens.
5. Enter a new QuickLoop name and click **OK**. The QuickLoop is renamed in the zoning database.

Creating a Fabric Assist Zone

The Mixed Zone level is used in this procedure

To create a fabric assist zone:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Select **View > Mixed Zoning**. You can select any view except for the Device view. The **Mixed View** tab is displayed.
3. Click the **Fabric Assist** tab.
4. Click **Create**. The Create New FA dialog box opens.
5. Enter a name for the new fabric assist zone and click **OK**. A fabric host is required.
6. Click the desired fabric assist zone members from the **Member Selection** list.
7. Click **Add Member**. The new members appear in the **Fabric Assist Members** area. The newly created fabric assist zone also is displayed in the **Config** tab.

Adding and Removing Fabric Assist Zone Members

To modify the members of a fabric assist zone:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Fabric Assist** tab.
3. From the **Name** menu, click the fabric assist zone you want to modify.
4. Click an element in the **Member Selection** list that you want to include in your fabric assist zone or click an element in the **Fabric Assist Zone Members** list that you want to delete.
5. Click **Add Member** to add a fabric assist zone member.
6. Click **Remove Member** to remove an fabric assist zone member.

Deleting a Fabric Assist Zone

To delete a fabric assist zone:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Fabric Assist Zone** tab.
3. From the **Name** menu, click the fabric assist zone you want to delete.
4. Click **Delete**. The Confirm Deleting Fabric Assist Zone dialog box opens.
5. Click **OK**. The selected fabric assist zone is deleted from the zoning database.

Renaming a Fabric Assist Zone

To rename a fabric assist zone:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Fabric Assist** tab.
3. From the **Name** menu, click the fabric assist zone you want to rename.
4. Click **Rename**. The Rename a Fabric Assist Zone dialog box opens.
5. Enter a new fabric assist zone name and click **OK**. The fabric assist zone is renamed in the zoning database.

Adding and Removing Zone Configuration Members

To add or remove the members of a zone configuration:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Config** tab.
3. From the **Name** menu, click the configuration you want to modify.
4. Click an element in the **Member Selection** list that you want to include in your configuration or click an element in the **Config Members** list that you want to delete.
5. Click **Add Member** to add a configuration member.
6. Click **Remove Member** to remove a configuration member.

Note: You can make changes to a configuration that is currently enabled; however, changes do not appear until the configuration is reenabled.

7. Select **Actions > Save Config Only**.

To enable the configuration, see “[Enabling a Zone Configuration](#)” on page 173.

Deleting a Zone Configuration

Note: You cannot delete a currently enabled configuration.

To delete a disabled configuration:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Config** tab.
3. From the **Name** menu, click the configuration you want to delete.
4. Click **Delete**. The Confirm Deleting Config dialog box opens.
5. Click **OK**. The selected configuration is deleted from the configuration database.

Renaming a Zone Configuration

To rename a configuration:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Config** tab.
3. From the **Name** menu, click the configuration you want to rename.
4. Click **Rename**. The Rename a Config dialog box opens.
5. Enter a new configuration name and click **OK**. The configuration is renamed in the configuration database.
6. Select **Actions > Save Config Only** to save the configuration changes.

To enable the configuration, see “[Enabling a Zone Configuration](#)” on page 173.

Creating a Configuration Analysis Report

To create a configuration analysis report:

1. Launch the Zone Administration module, as described in “[Accessing the Zone Administration Module](#)” on page 169.
2. Click the **Config** tab.
3. From the **Name** menu, click a configuration to be analyzed.
4. Click **Analyze Config**. A dialog box opens, asking whether you want to refresh the fabric before running the analysis.
5. Click **Yes** or **No**. An analysis window is displayed.
6. Review the configuration analysis, which lists:
 - SAN components (ports, WWNs, and AL_PAs) that are not included in the configuration.
 - SAN components (ports, WWNs, and AL_PAs) that are contained in the configuration, but not in the fabric.

Zoning Reference

This reference provides information about zoning fields. It describes the components of the Zone Administration interface. [Table 28](#) explains the components of the Zone Administration window.

Note: Zoning interfaces vary by firmware. Your interface might appear differently.

Table 28: Zone Administration Window Components

Component	Description
File menu	Provides administrative options. For more information on the items in this menu, see "File Menu" on page 183.
Edit menu	Lets you add, delete, replace, and search for zone member identifiers. For more information, see "Edit Menu" on page 184.
View menu	Lets you choose a zoning display. For more information, see "View Menu" on page 184.
Actions menu	Lets you enable, disable, and save zoning configurations. For more information, see "Actions Menu" on page 185.
Zoning type display	Displayed beneath the File menu and displays the zoning type that you chose from the View menu.
Enabled config display	Displayed the enabled zoning configuration.
Zoning configuration tabs	Let you configure zoning. For more information, see the tab-specific sections that follow: <ul style="list-style-type: none"> ■ "Alias Tab" on page 185 ■ "Zone Tab" on page 187 ■ "QuickLoop Tab" on page 189 ■ "Fabric Assist Tab" on page 190 ■ "Config Tab" on page 192

File Menu

[Table 29](#) describes the options that appear in the **File** menu of the Zone Administration window.

Table 29: File Menu Options

Option	Description
Print Summary	Select to print a zoning configuration report. A window displays both the effective configuration and the defined zoning configuration, if one exists.
Close	Select to close the Zone Administration window.

Edit Menu

Table 30 describes the options that appear in the **Edit** menu of the Zone Administration window.

Table 30: Edit Menu Options

Option	Description
Add WWN	Select to add a WWN across aliases, zones, or fabric assist zones. A dialog box opens; enter the WWN number.
Delete WWN	Select to delete a WWN across aliases, zones, or fabric assist zones. A dialog box opens; enter the WWN number.
Replace WWN	Select to replace one WWN with another. A dialog box opens; enter first the WWN number to be replaced, and then the new WWN number.
Search Member	<p>Select to search for a member of a zone. A dialog box opens; enter any element that is displayed in the Member Selection list: Domain Name, Port name, Port ID, WWN, Device, Zone Name, or Alias Name.</p> <p>Narrow searches by checking one or more of the following check boxes:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Match Case <input type="checkbox"/> Match whole words only <input type="checkbox"/> Wrap around. <p>Check the Wrap around box if you want the search engine to restart after it hits the end of the string. Leave unchecked if you want the search engine to stop after it hits the end of the string; a message is displayed to indicate the search is complete.</p>

View Menu

The options available in the **View** menu of the Zone Administration window are described in Table 31.

Table 31: View Menu Options

Option	Description
Mixed Zoning	Use the Mixed Zoning option when you want to include various objects as member of an alias, zone, or configuration file.
Port Zoning	Select the Port Zoning option when you want to include only ports in a group. Grouping zones by port alone constitutes hard zoning.
WWN Zoning	Select the WWN Zoning option when you want to zone by WWNs. Grouping zones by WWN alone constitutes hard zoning.
AL_PA Zoning	Select the AL_PA Zoning option when you want to create or manage a zone of devices.
Refresh Zoning	Select the Refresh Zoning option to refresh the zoning database. This overwrites any unsaved zoning database changes you have made.
Refresh Fabric	Select the Refresh Fabric option to display the latest fabric changes.

Actions Menu

The options available in the **Actions** Menu of the Zone Administration window are described in [Table 32](#).

Table 32: Actions Menu Options

Menu Item	Description
Enable Config	Select to save and enable the configuration selected from the Config tab Name field. This command also saves all other configurations in the zoning database.
Disable Zoning	Select to disable the configuration that is currently enabled. A dialog box provides a warning before disabling.
Save Config Only	Select to save all defined zoning configurations. The saved changes apply only to the defined configurations. Changes can be made to a configuration that is currently enabled; changes do not appear until the configuration is disabled and reenabled.
Clear All	Select to delete all aliases, zones, fabric assist zones, and configurations; the cleared configuration is saved. Any enabled configuration is disabled.

Alias Tab

Use the **Alias** tab to create, modify, rename, or delete aliases in the zoning database. An example of the **Alias** tab is shown in [Figure 39](#).

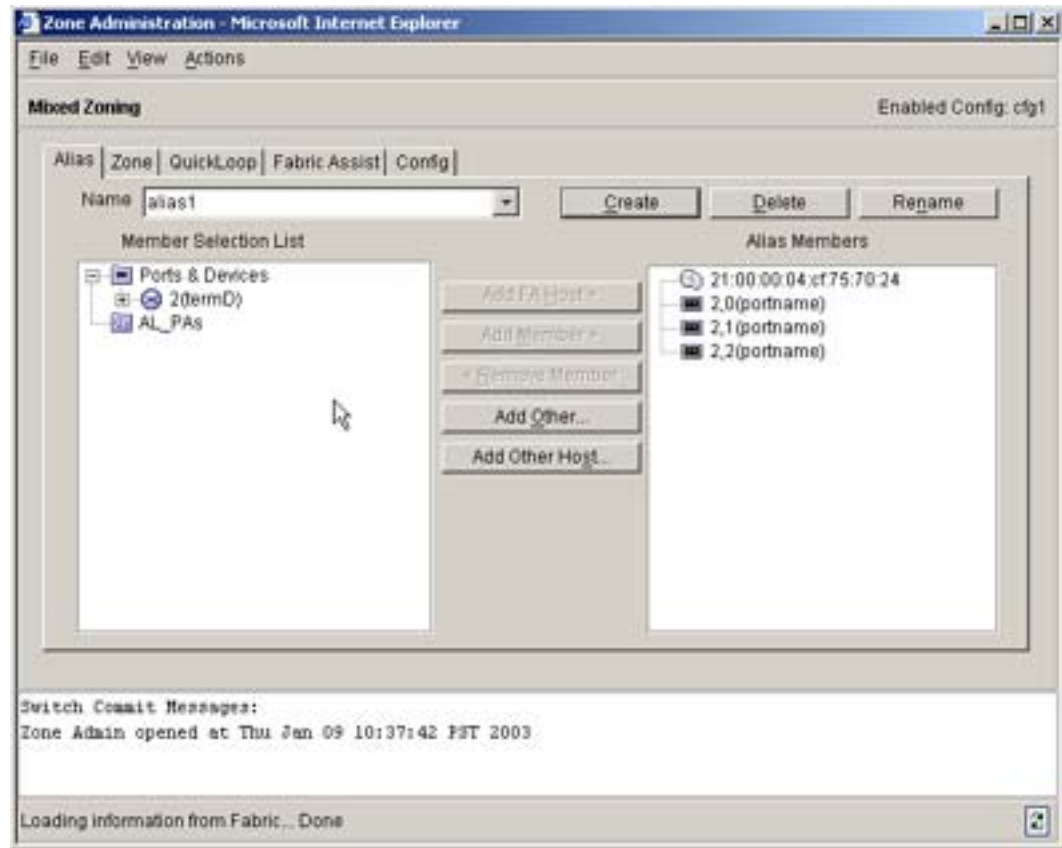


Figure 39: Alias Tab in the Zone Administration Window

Alias Tab Descriptions

Table 33 explains the components of the **Alias** tab.

Table 33: Alias Tab Component Descriptions

Component	Description
Name pull-down menu	Displays existing alias names from the pull-down menu.
Create button	Click to create a new alias. A dialog box opens. Enter the name of the new alias. All names must be unique and contain no spaces.
Delete button	Click to delete the alias selected in the Name field. Deleting an alias automatically removes it from all zones and configurations.
Rename button	Click to rename the alias selected in the Name field. A dialog box opens in which you can rename the alias. Renaming an alias automatically renames it in all zones and configurations.
Member Selection list	Use to select available items from the Member Selection list. In mixed zones, you can select Ports, WWNs, and AL_PAs.
Alias Members field	Displays the current members of an alias.
Add FA Host button	Click to add a Fabric Assist host to the member list.
Add Member button	Click to add a member from the Member Selection list to the Alias Members field. You must select a member within Member Selection list for this button to become active.
Remove Member button	Click to remove a member from the Alias Members list. You must select a member within the Alias Members list for this button to become active.
Add Other button <ul style="list-style-type: none"> ■ Other ■ Other Port ■ Other WWN ■ Other AL_PA 	Click to add a port, WWN or AL_PA that is not currently part of the fabric. A dialog box opens. Enter the host name that is not a member of the fabric.
Add Other Host button <ul style="list-style-type: none"> ■ Other Host ■ Other Port Host ■ Other WWN Host 	Click to add a host that is not currently part of the fabric. The button displayed depends on the zoning method that you have selected.

Zone Tab

Use the **Zone** tab to create, modify, rename, or delete zones in the zoning database. An example of a **Zone** tab is shown in [Figure 40](#).

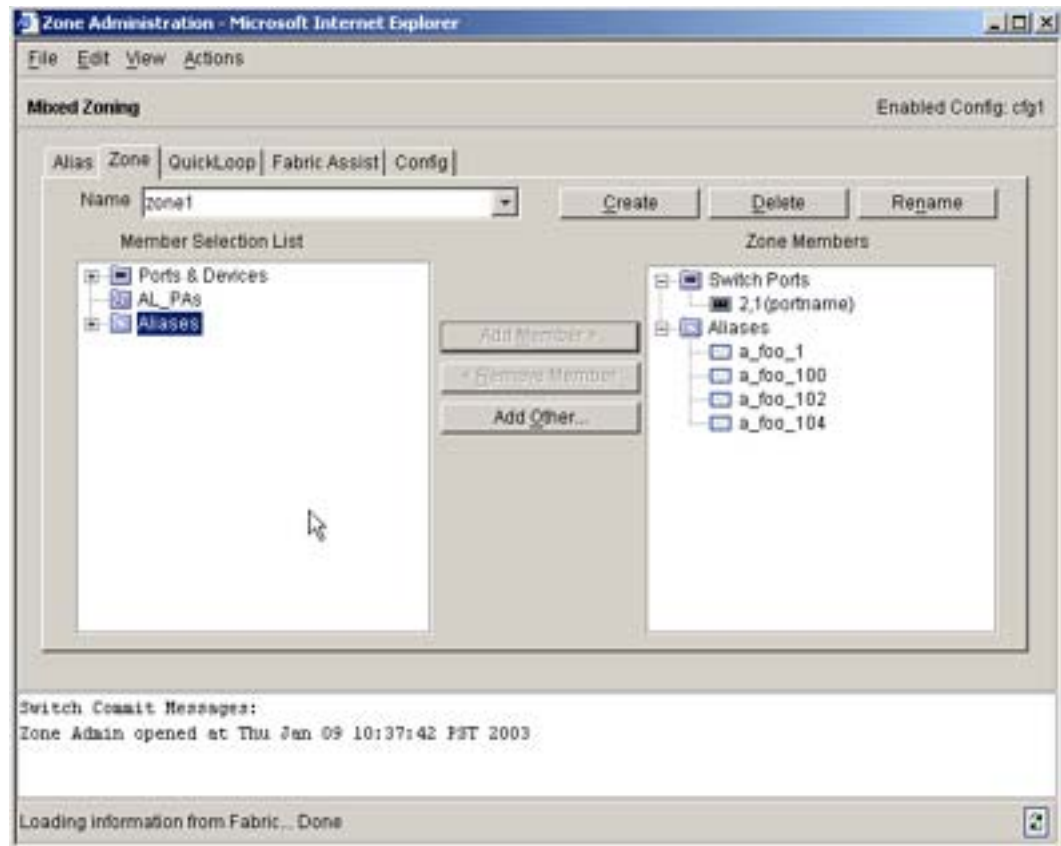


Figure 40: Zone Tab in the Zone Administration Window

Zone Tab Descriptions

Table 34 explains the components of the **Zone** tab.

Table 34: Zone Tab Component Descriptions

Component	Description
Name pull-down menu	Displays existing zones from the pull-down menu.
Create button	Click to create a new zone. A dialog box opens. Enter the name of the new zone. All zone names must be unique and must consist of letters, numerals, or the underscore character. Spaces and special characters are not allowed in zone names. A name cannot start with a numeral.
Delete button	Click to delete the zone selected in the Name field. Deleting a zone removes it from all configurations.
Rename button	Click to rename the Zone selected in the Name field. A dialog box opens in which you can edit the zone name. Renaming a zone in the Zone tab renames it in all configurations.
Member Selection list	Select available items from the Member Selection list.
Zone Members field	Displays the current members of a zone.
Add Member button	Click to add a member from the Member Selection list to the Zone Members field. You must select a member within the Member Selection list for this button to become active.
Remove Member button	Click to remove a member from the Zone Members list. You must select a member within the Zone Members list for this button to become active.
Add Other <ul style="list-style-type: none"> ■ Other Port ■ Other WWN ■ Other AL_PA 	Click to add a port, WWN or AL_PA that is not currently part of the fabric. A dialog box opens. Enter the host name that is not a member of the fabric.

QuickLoop Tab

Use the **QuickLoop** tab to manage QuickLoops in the zoning database. For more information regarding QuickLoops, refer to your firmware documentation. An example of the **QuickLoop** tab is shown in [Figure 41](#).

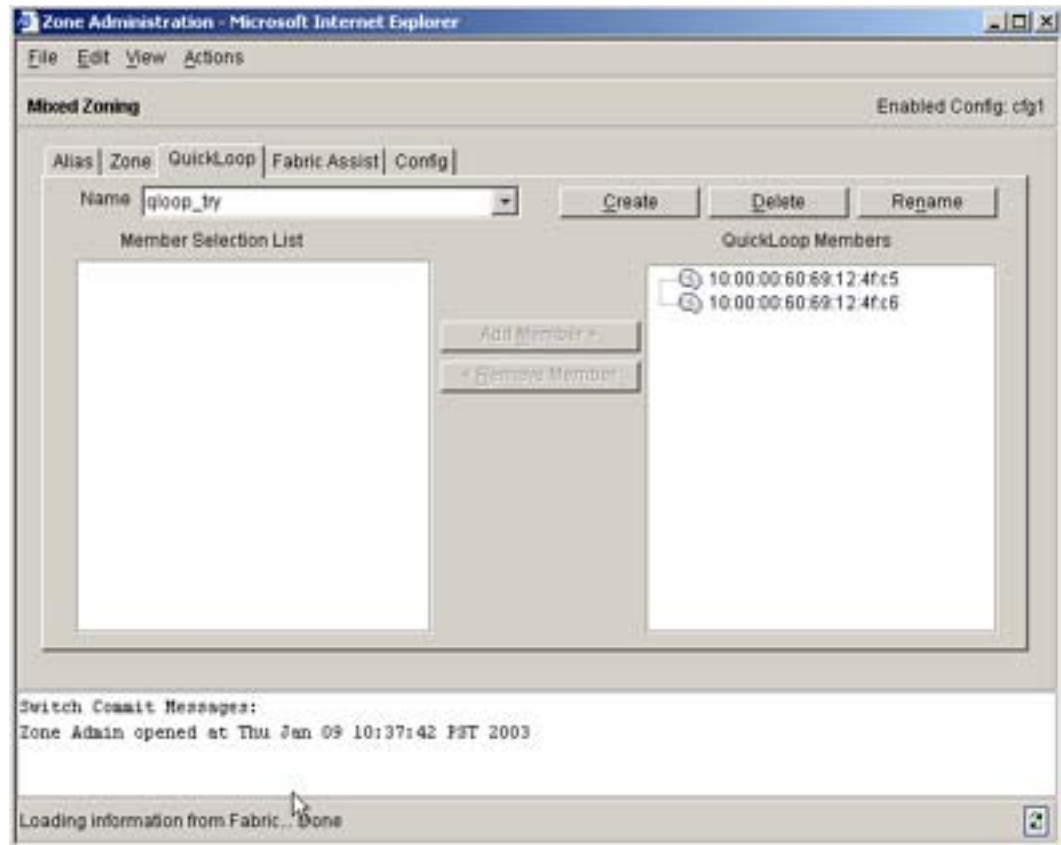


Figure 41: QuickLoop Tab in the Zone Administration Window

QuickLoop Tab Descriptions

Table 35 explains the components of the **QuickLoop** tab.

Table 35: QuickLoop Tab Component Descriptions

Component	Description
Name pull-down menu	Displays existing QuickLoops.
Create button	Click to create a new QuickLoop. A dialog box opens. Enter the name of the new QuickLoop. All names must be unique and contain no spaces.
Delete button	Click to delete the QuickLoop selected in the Name pull-down menu. Deleting a QuickLoop removes it from all configurations.
Rename button	Click to rename the QuickLoop selected in the Name pull-down menu. A dialog box opens in which you can edit the QuickLoop name. Renaming a QuickLoop renames it in all configurations.
Member Selection list	Select available members from the Member Selection list. QuickLoop is not supported on switches that run firmware versions 4.x. However, you can manage a QuickLoop from these switches if it is attached to another switch in the fabric.
QuickLoop Members field	Displays the current members of a QuickLoop.
Add Member button	Click to add a member from the Member Selection list to the QuickLoop Members field. You must select a member within the Member Selection list for this button to become active.
Remove Member button	Click to remove a member from the QuickLoop Members field. You must select a member within QuickLoop Members field for this button to become active.

Fabric Assist Tab

Use the **Fabric Assist** tab to create and manage fabric assist zones. Fabric Assist allows private hosts to communicate with public targets across a switched fabric. Fabric Assist also allows private hosts to communicate with public targets that do not reside on the same switch.

You cannot create a fabric assist zone without a fabric host. You cannot access the **Fabric Assist** tab if you selected **View > AL_PA Zoning**. Figure 42 is an example of a **Fabric Assist** tab.

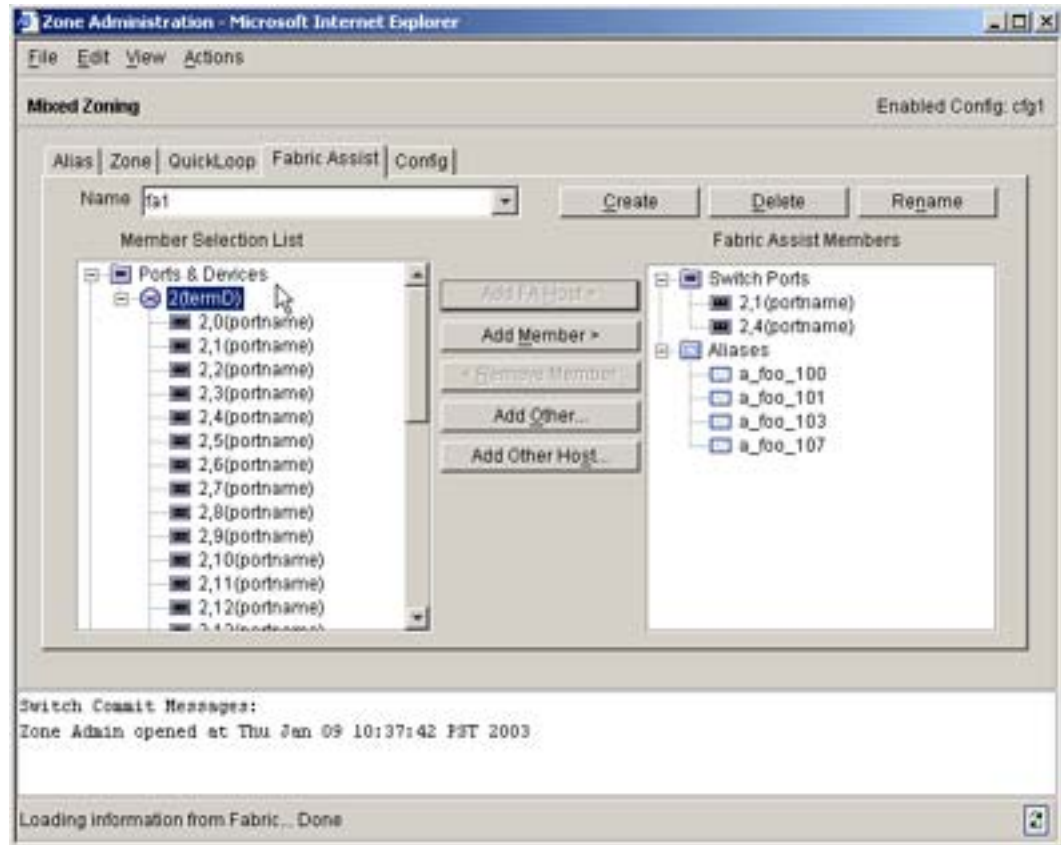


Figure 42: Fabric Assist Tab in the Zone Administration Window

Fabric Assist Tab Descriptions

Table 36 explains the components of the **Fabric Assist** tab.

Table 36: Fabric Assist Component Descriptions

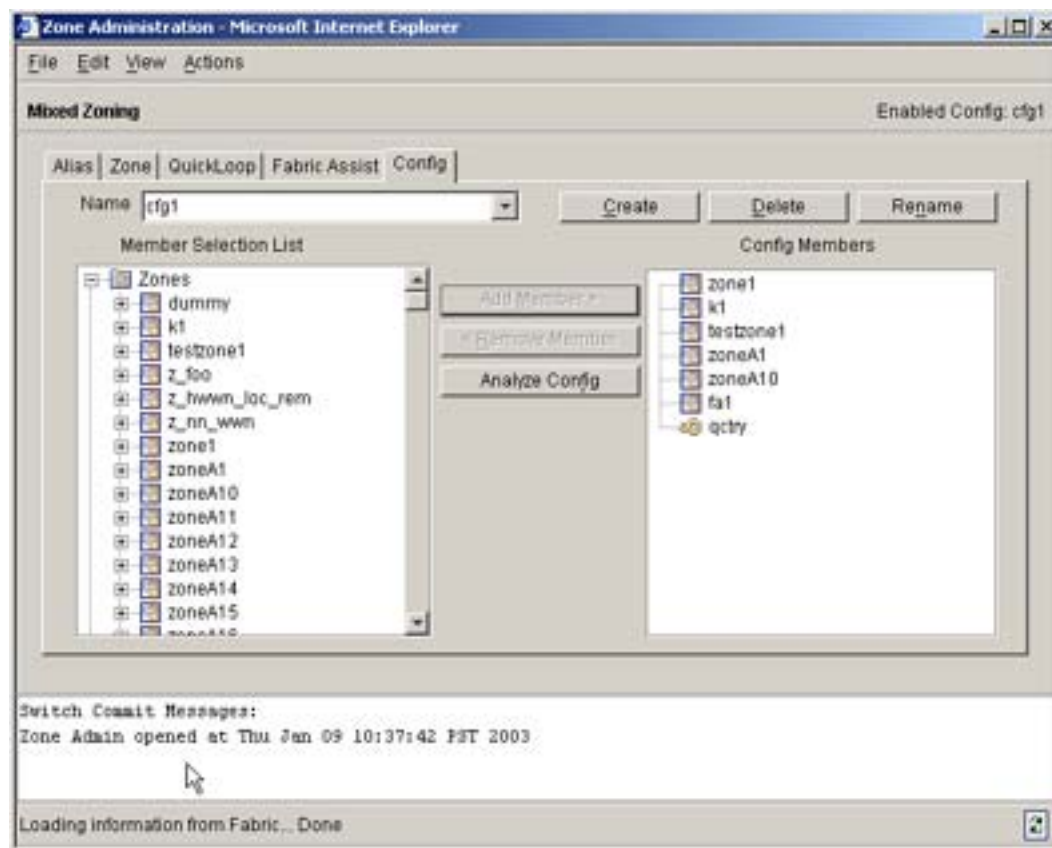
Component	Description
Name pull-down menu	Displays existing fabric assist zones from the pull-down menu.
Create button	Click to create a new fabric assist zone. A dialog box opens. Enter the name of the new fabric assist zone. All names must be unique and contain no spaces.
Delete button	Click to delete the fabric assist zone selected in the Name pull-down menu. Deleting a fabric assist zone removes it from configurations.
Rename button	Click to rename the fabric assist zone selected in the Name pull-down menu. A dialog box opens in which you can edit the fabric assist name. Renaming a fabric assist zone renames it in all configurations.
Member Selection list	Select available items from the Member Selection list.
Fabric Assist Members field	Displays the current members of an fabric assist zone.
Add FA Host button	Click to add a Fabric Assist host that is not currently part of the fabric.
Add Member button	Click to add a member from the Member Selection list to the Fabric Assist Members field. You must select a member within Member Selection list for this button to become active.

Table 36: Fabric Assist Component Descriptions (Continued)

Component	Description
Remove Member button	Click to remove a member from the Fabric Assist Members list. You must select a member within Fabric Assist Members field for this button to become active.
Add Other button <ul style="list-style-type: none"> ■ Other ■ Other Port ■ Other WWN ■ Other AL_PA 	Click to add a fabric assist zone that is not currently part of the fabric. A dialog box displays. Enter the host name that is not a member of the fabric.
Add Other Host button <ul style="list-style-type: none"> ■ Other Host ■ Other Port Host ■ Other WWN Host 	Click to add a host that is not currently part of the fabric. The button displayed depends on the zoning method that you have selected.

Config Tab

Use the **Config** tab to create and manage configurations. An example of the **Config** tab is shown in [Figure 43](#).

**Figure 43: Config Tab in the Zone Administration Window**

Config Tab Descriptions

Table 37 explains the components of the **Config** tab.

Table 37: Config Tab Component Descriptions

Component	Description
Name pull-down menu	Select an existing configuration from the pull-down menu to display or modify.
Create button	Click to create a new configuration. A dialog box opens. Enter the name of the new configuration. All names must be unique and contain no spaces.
Delete button	Click to delete the configuration selected in the Name pull-down menu. Deleting a configuration does not delete any of the elements contained in that configuration.
Rename button	Click to rename the configuration selected in the Name pull-down menu. A dialog box opens in which you can edit the configuration name.
Member Selection List field	Select available items from the Member Selection list.
Config Members field	Displays the current config members.
Add Member button	Click to add a member from the Member Selection list to the Config Members field. You must select a member within Member Selection list for this button to become active.
Remove Member button	Click to remove a member from the Config Members list. You must select a member within Config Members field for this button to become active.
Analyze Config button	Analyzes the configuration that is selected along with its member zones. A report is created that lists: <ul style="list-style-type: none"> ■ SAN components (ports, WWNs, and AL_PAs) that are not included in the configuration. ■ SAN components (ports, WWNs, and AL_PAs) that are contained in the configuration but not in the fabric.

Troubleshooting

22

This chapter describes a few problem scenarios that can occur while using Fabric Manager and provides troubleshooting tips to help you resolve these problems. See the following sections for troubleshooting information specific to the suspected trouble area:

- [“Checking Fabric Manager”](#) on page 196
- [“Checking the Client Side”](#) on page 196
- [“Checking Client/Server Interaction”](#) on page 198
- [“Checking the Server Side”](#) on page 199
- [“Checking Fabric Discovery Problems”](#) on page 199
- [“Saving the SupportShow Command Output”](#) on page 201
- [“Pinpointing Additional Problem Areas”](#) on page 202

Checking Fabric Manager

In the following procedure, the destination directory (*destdir*) must already exist before you run the script. The `fmsupportshow` scripts for both Windows and Solaris then provide the following information in the specified destination directory:

- Fabric Manager (client-only installation): `client` directory with client debug information (including logs, system information, and so on).
- Fabric Manager (server-only installation): `server` directory with server debug information (including logs, database, system information, and so on).
- Fabric Manager (client and server installation): `client` and `server` directory with all of the client and server debug information.

For all problems with Fabric Manager, follow these steps:

1. Run the following script to capture the problem:
For Windows: `installdir/bin/fmsupportshow.bat destdir`
For Solaris: `installdir/bin/fmsupportshow.sh destdir`
Scripts are located in the `$FM_HOME/bin` directory.
2. Obtain a screen shot of the client (if you are reporting a GUI problem).
3. Include any fabric or switch activities: firmware downloads, reboots, segmentation, merge, and the like.
4. Include any actions executed from Fabric Manager.
5. Report the problem to technical support (via `.zip` or `tar` file).

Checking the Client Side

If you suspect the problem is related to the client side, use the procedures in the following sections:

- [“Authentication Issues \(Unable to Log in\)”](#) on page 196
- [“Client Access to Switches”](#) on page 197
- [“Client-Side CPU Usage”](#) on page 197

If the problem persists or cannot be resolved, see [“Capturing and Reporting Client-Side Issues”](#) on page 197.

Authentication Issues (Unable to Log in)

If the user is unable to log in to the Fabric Manager server, follow these steps:

1. Check the userid and password.
2. Check the login module and domain settings in the server:

```
installdir/server/server/fmserver/deploy/fmauth-service.xml
```

Depending on the platform you have installed, there are three possible valid settings within the `fmauth-service.xml` file:

- Fabric Manager server running under Windows when using Windows domain authentication (this is the only supported Windows authentication mechanism):

```
attribute name="LoginModule"Win/attribute
attribute name="DomainName" "your_domain"/attribute
```

- Fabric Manager server running under Solaris when using NIS authentication:

```
attribute name="LoginModule"NIS/attribute
attribute name="DomainName"yourdomain.com/attribute
attribute name="NISServer""your_NISServer"/attribute
```

- Fabric Manager server running under Solaris when using local password authentication:

```
attribute name="LoginModule"File/attribute
```

Note: If you are using the local password authentication, the *DomainName* attribute is missing from the XML file. Also, if you are using the NIS authentication, there is an extra parameter in the XML file called *NISServer*.

3. Check the Fabric Manager server log for any errors:

```
installdir/server/server/fmserver/log/server.log
```

Example

```
2004-05-27 17:11:19,256 INFO
[com.hp.fabman.auth.server.FMAuthRemoteServer] Creating New Login
Session: user = [stsun], client host = [192.168.42.139], session id= [2]
2004-05-27 17:11:19,272 INFO
[com.hp.fabman.auth.server.WinNTLoginModule] Authenticating user
[stsun] using [hp] domain
2004-05-27 17:11:20,272 ERROR
[com.hp.fabman.auth.server.WinNTLoginModule] Authentication failed for
[hp/stsun]
```

Client Access to Switches

If the client cannot access some of the switches, you need to check the IP connectivity between the client/server, the client/switch, and the server/switch; then, check the web server on the switch by invoking Advanced Web Tools on that switch.

Client-Side CPU Usage

If the client-side CPU usage is too heavy and has an unusually sluggish or slow response, check the recommended configuration.

Capturing and Reporting Client-Side Issues

If you cannot resolve the problem but know it is a client-side issue, follow these steps:

1. Run the following script to capture the problem:

For Windows: `installdir/bin/fmclientsupportshow.bat destdir`

For Solaris: `installdir/bin/fmclientsupportshow.sh destdir`

Scripts are located in the `$FM_HOME/bin` directory.

Note: Use the `fmsupportshow.bat` script (for Windows) or `fmsupportshow.sh` script (for Solaris) to collect all required data for a Fabric Manager installation on a host. See [“Checking Fabric Manager”](#) on page 196 for additional information.

2. Obtain a screen shot of the client (if you are reporting a GUI problem).
3. Include any fabric or switch activities: firmware downloads, reboots, segmentation, merge, and the like.
4. Include any actions executed from Fabric Manager.
5. Report the problem to technical support (via .zip or tar file).

Checking Client/Server Interaction

If you suspect the problem is related to an interaction between the client and the server, use the procedures in the following sections:

- [“No Client/Server Interaction”](#) on page 198
- [“Client/Server Version Mismatch”](#) on page 198
- [“Determine Client or Server Problem”](#) on page 198

No Client/Server Interaction

If the client cannot talk to the server, follow these steps:

1. Ensure that the server name is correct.
2. Ensure that the port number is correct.
3. Ensure there is IP connectivity (ping, traceroute, and so on).
4. Check for the presence of firewalls.
5. If a firewall is present, ensure that the proper ports are opened.

Fabric Manager takes the first six ports (numerically) starting with the port entered during the installation. For example, if you entered 24600 as the port during the installation, ports 24600 through 24605 are included. Also, for HTTP and API purposes, ports 80, 111, and 600 through 1023 are automatically used too.

Client/Server Version Mismatch

If the client has an incompatible version, a warning is issued. Upgrade the component (client or server) with the earlier version.

Determine Client or Server Problem

To determine whether the problem is related to the client or the server, follow these steps:

1. Run another client.
If the other client displays correct data, the problem is probably client-related. If it displays incorrect data, the problem is probably associated with the server.
2. Check the server log for any errors. If errors exist, it is probably a server problem if the client is operating incorrectly.

Checking the Server Side

If you suspect the problem is related to the server side, use the procedures in the following sections:

- [“Server Cannot Access Switches”](#) on page 199
- [“Server-Side CPU Usage”](#) on page 199

If the problem persists or cannot be resolved, see [“Capturing and Reporting Server-Side Issues”](#) on page 199.

Server Cannot Access Switches

If the server cannot access any switches, follow these steps:

Note: Fabric Manager displays inaccessible switches with a blue icon.

1. Ensure that there is IP connectivity to the switches.
2. If you are running secure Fabric OS, check `http_policy`.
3. Ensure the version of the Fabric OS is supported.

Server-Side CPU Usage

If the server side CPU usage is too heavy and has an unusually sluggish or slow response, check the recommended configuration.

Capturing and Reporting Server-Side Issues

If you cannot resolve the problem, but know it is a server side issue, follow these steps:

1. Run the following script to capture the problem:
For Windows: `installdir/bin/fmserversupportshow.bat destdir`
For Solaris: `installdir/bin/fmserversupportshow.sh destdir`
Scripts are located in the `$FM_HOME/bin` directory.
2. Report the problem to technical support.

Note: Use the `fmsupportshow.bat` script (for Windows) or `fmsupportshow.sh` script (for Solaris) to collect all required data for a Fabric Manager installation on a host. See [“Checking Fabric Manager”](#) on page 196 for additional information.

Checking Fabric Discovery Problems

If you are having fabric discovery problems, identify the problem (see below) and try the recommended solution:

- If the switch does not exist or there is no Ethernet path to the switch, attempt to ping the switch from both the client and the server.
- If the IP address is not properly formed, fix the IP address and/or URL.

- If the domain name is unknown to the DNS, check the DNS configuration.
- If HTTP service on the switch is not running (or is running too slow), attempt to use Advanced Web Tools via the client.
- If the fabric was reconfiguring or unstable at the time of the attempted launch, use the `fabricshow` command to determine whether the fabric is stable.
- If the switch does not have an Advanced Web Tools license, try to use Advanced Web Tools via the client host.
- If the switch cannot deliver `Fabricinfo.html`, it is not an HP StorageWorks switch.
- If the launch switch is already monitored in another fabric, check all of the loaded fabrics on the client GUI.
- If the client has lost connection to the server (or server is down):
For Windows, from the **Start** menu, select **Settings > Control Panel > Administrative Tools > Services > Fabric Manager Server** (see [Figure 44](#)). Then use the **Action** menu to reconnect accordingly.
- If the database is not running:
For Windows, from the **Start** menu, select **Settings > Control Panel > Administrative Tools > Services > Adaptive Server Anywhere - fabmandb** (see [Figure 45](#)). Then use the **Action** menu to start or restart the database.

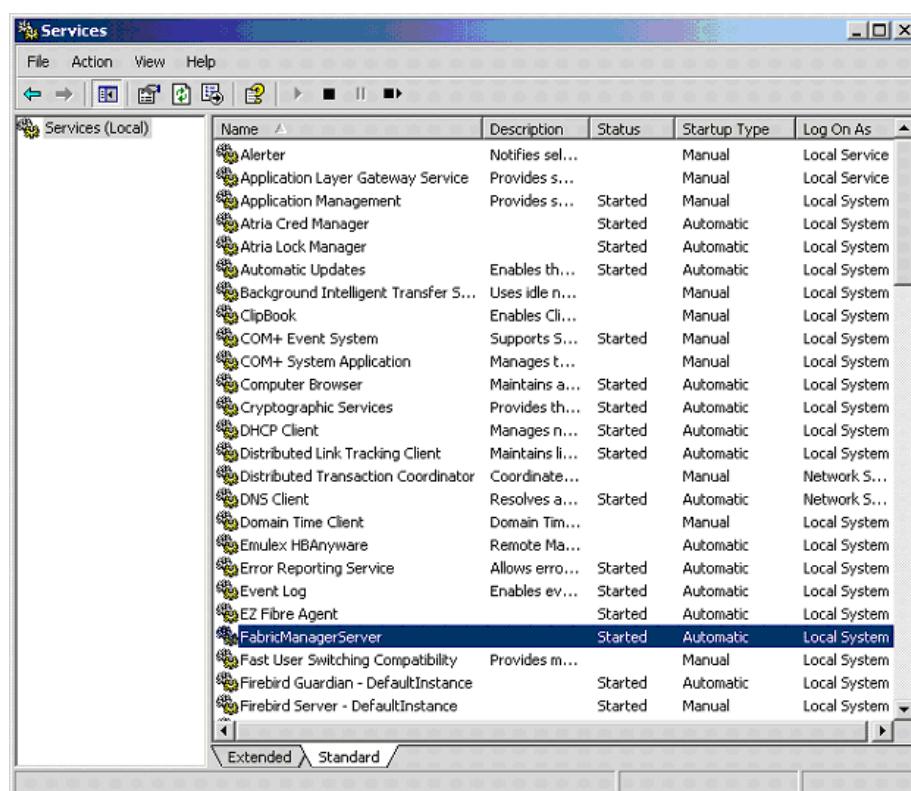


Figure 44: Fabric Manager Server (Services Window)

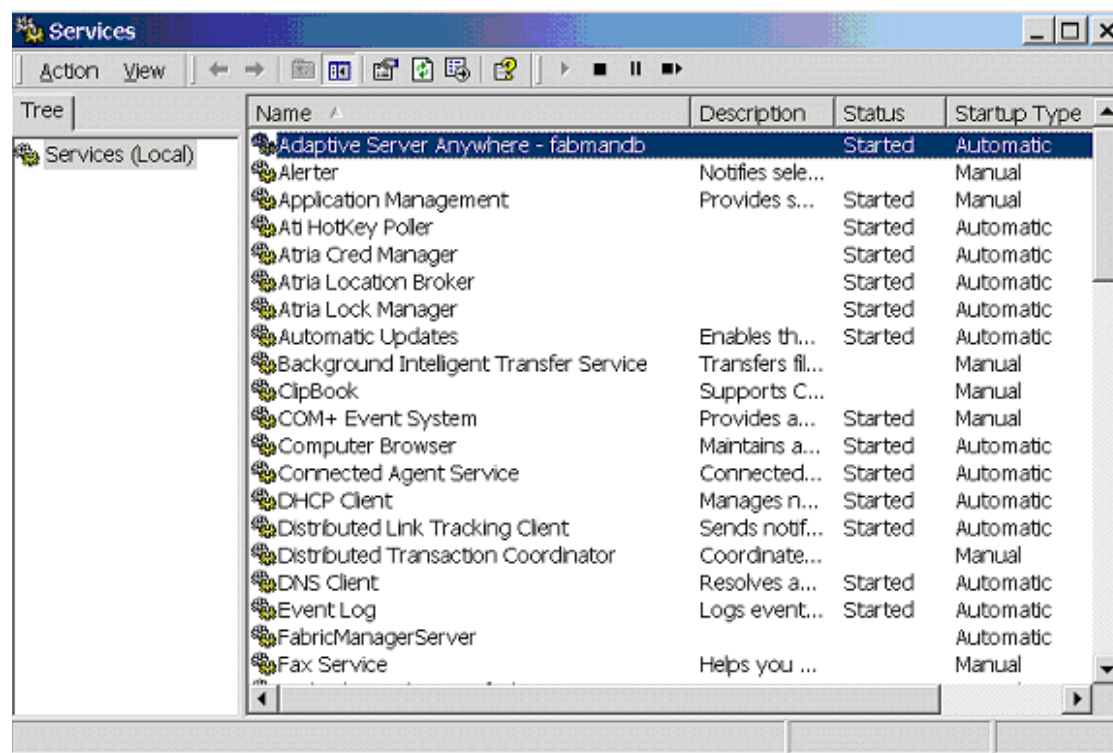


Figure 45: Database (Services Window)

Saving the SupportShow Command Output

If a switch is not operating as expected, use the `supportshow` command to capture diagnostic data for the switch. You can use Fabric Manager to save the `supportshow` command output as a text file that you can troubleshoot yourself or send to your technical support contact for analysis. For multiple switches, multiple text files are created, one for each switch, and are archived together into a single `.zip` file.

To print the `supportshow` command output:

1. Click a switch from the **SAN Elements** tab.
2. Select **Actions > Supportshow**. A Save dialog box opens.
3. Enter a name for the file, and select a location where you want to save the file.

Pinpointing Additional Problem Areas

This section describes specific problems that you may experience with Fabric Manager. A solutions to the problems are included.

Installing Fabric Manager Client on Solaris Using BASH as Default Shell

When installing the Fabric Manager client on a Solaris 8 OS with a BASH as the default shell, you must run the following command from the command line before launching the Fabric Manager client:

```
bash --login
```

If you do not run this command before launching the client, Fabric Manager does not run properly.

Cannot Locate Fabric Manager License Key and Serial Number

Fabric Manager v4.1.0 and later stores the serial number and license key in a file each time a user successfully registers Fabric Manager. The file name is `fmlicense.txt` and should be in the local `Fabric Manager user` directory. The file contains the version of Fabric Manager installed, the serial number, license key, license type, and licensing date. If you cannot locate the file, contact Technical Support.

Switches and Hosts No Longer Recognize an HBA After Firmware Download to HBA

During the firmware-download-to-HBA process, if the switch (that the HBA is attached to) is rebooted or the host (that the HBA is attached to) is rebooted, the firmware in the HBA flash memory can become corrupted and HBA is not able to log in to the switch or respond to the query from the switch. Thus, from both the Fabric Manager and the switch point of view, this HBA does not appear and drops out of the name server list. To solve this problem, use HBAnyware on the attached host and reload the firmware on the HBA.

503 Service Unavailable/Overloaded Error

The 503 error indicates that Fabric Manager has discovered a switch whose web server is unavailable or overloaded. If you receive this error, try to poll the switch using only one Fabric Manager server.

When a switch displays this error after Fabric Manager has already discovered the switch, the error is displayed only in the error log.

Although switches can appear as unreachable in Fabric Manager when they receive this error, the error occurs more frequently on switches that run firmware versions 2.x and 3.x.

Installation Wizard Does Not Launch

Run the DOS command `dxdiag` and make sure that the graphics tests run without errors. If any version of DirectX files or any diagnostic files are missing, go to the Microsoft® Web site and upgrade to the latest version of DirectX.

Installation Wizard Locks Up

Press the **Ctrl** key until a DOS Java console is displayed. The console captures a log of the entire installation process.

Incorrect Performance Monitoring Port Statistics

If you are running a 4.x version of Fabric OS on a switch that is v4.2.0b or earlier, the Advanced Performance Monitoring port statistics for it are returned incorrectly. You must upgrade the firmware on the 4.x switch to Fabric OS v4.2.0c or later.

File Menu Reference



This appendix consists of the following sections:

- [“Introduction”](#) on page 205
- [“Fabric Login Window”](#) on page 206
- [“Groups Submenu”](#) on page 207
- [“Options Window”](#) on page 208

Introduction

The **File** menu in Fabric Manager provides basic administrative options. [Table 38](#) describes the options in the **File** menu.

Table 38: File Menu Options

Option	Description
New	Opens a new Fabric Manager window. All other Fabric Manager windows remain open.
Close	Closes the active Fabric Manager window. This option is available only when you open multiple Fabric Manager windows.
Fabric Login	Opens the Fabric Login window to log in to multiple switches. For more information, see “Fabric Login Window” on page 206.
Groups	Opens the Groups submenu so you can create, edit, import, and export switchgroups and portgroups. For more information on the Groups submenu, see “Groups Submenu” on page 207.
Options	Opens the Options window to set default options for the following areas: <ul style="list-style-type: none">■ Topology■ Fabric change■ ISL status■ Log parameters■ File transfers For more information, see “Options Window” on page 208.
Print	Opens the Print window to print a report summary or topology.
Print In One Page	Opens the Print window to print a topology on one page.
Page Setup	Opens the Page Setup window to configure print options.
Exit	Closes Fabric Manager.

Fabric Login Window

The Fabric Login window lets you log in to multiple switches simultaneously. [Table 39](#) explains the components of the window.

For instructions that explain how to perform a fabric login, see “[Logging In to Multiple Devices Simultaneously](#)” on page 48.

Table 39: Fabric Login Window Components

Component	Description
User ID field	Accepts the user ID that you use to log in to the switches.
Password field	Accepts the password that you use to log in to the switches.
Name, IP, WWN radio buttons	Determines how the SAN Elements tab identifies switches. For more information, see “ Displaying SAN Elements by IP address, Domain ID, WWN, and Name ” on page 50.
SAN Elements tab	Displays the fabrics, switches, and groups that you can log in to.
Filter tab	Filters elements based on alphanumeric text strings.
directional arrows	Adds or removes switches from the Selected Switches field.
Selected Switches field	Displays the switches that you have chosen to log in to.
IP Address column	Displays the IP address of each switch in the Selected Switches field. Click the column header to list all switches in ascending or descending order by IP address.
Switch Name column	Displays the switch name of each switch in the Selected Switches field. Click the column header to list all switches in ascending or descending order by switch name.
Firmware version column	Displays the firmware that runs on each switch in the Selected Switches field. Click the column header to list all switches in ascending or descending order by firmware version.
UserID column	Displays the user ID that you used to log in to each switch in the Selected Switches field. If you have not logged in to the switch, this field is blank. Click the column header to list all switches in ascending or descending order by user ID.
Status column	Displays the log in status of each switch in the Selected Switches field. Click the column header to list all switches in ascending or descending order by status.
Apply button	Applies the user ID and password that you specify to log in to one or more switches.
Close button	Closes the Fabric Login window.
Help button	Opens Fabric Manager Help.

Groups Submenu

The **Groups** submenu lets you configure, import, and export Fabric Manager logical groups. [Table 40](#) explains the options in this submenu.

Table 40: Groups Submenu Items

Option	Description
Edit Switch Groups	Opens the Edit Switch Groups window to create or modify switch groups. For information on the window, see “Edit Switch Groups Window” on page 207.
Edit Port Groups	Opens the Edit Port Groups window to create or modify port groups. For information on the window, see “Edit Port Groups Window” on page 208.

Edit Switch Groups Window

The Edit Switch Groups window lets you create new switch groups and modify or delete existing switch groups. [Table 41](#) explains the components of the window.

Table 41: Edit Switch Groups Window Components

Component	Description
Name, IP, WWN radio buttons	Determines how the SAN Elements tab identifies switches. For more information, see “Displaying SAN Elements by IP address, Domain ID, WWN, and Name” on page 50.
SAN Elements tab	Displays the fabrics and switches that you can add to your groups.
Filter tab	Filters elements based on alphanumeric text strings.
SwitchGroups navigation tree	Displays existing switch groups and lets you move groups within the tree.
Create button	Opens the Create Group window to create and name a new switch group.
Edit button	Opens the Edit Group window to rename an existing switch group.
Delete button	Deletes an existing switch group.
OK button	Applies and saves switch group edits.
Cancel button	Aborts switch group edits.
Help button	Opens Fabric Manager Help to the Groups section.

Edit Port Groups Window

The Edit Port Groups window lets you create new port groups and modify or delete existing port groups. [Table 42](#) explains the components of the window.

Table 42: Edit Port Groups Window Components

Component	Description
Name, IP, WWN radio buttons	Determines how the SAN Elements tab identifies switches. For more information, see “Displaying SAN Elements by IP address, Domain ID, WWN, and Name” on page 50.
SAN Elements tab	Displays the fabrics and switches that you can add to your groups.
Filter tab	Filters elements based on alphanumeric text strings.
PortGroups navigation tree	Displays existing port groups and lets you move groups within the tree.
Create button	Opens the Create Group window to create and name a new port group.
Edit button	Opens the Edit Group window to rename an existing port group.
Delete button	Deletes an existing port group.
OK button	Applies and saves port group edits.
Cancel button	Aborts port group edits.
Help button	Opens Fabric Manager Help to the Groups section.

Options Window

The Options window lets you configure various Fabric Manager defaults. The Configurations navigation tree displays the categories of options that you can configure. [Table 43](#) explains the categories of options that you can configure.

Table 43: Options Categories

Category	Description
Switch Passwords	Allows you to enable switch passwords to remain persistent across reboots.
Topology	<p>Lets you configure the following defaults:</p> <ul style="list-style-type: none"> ■ Default Startup Layout ■ Default Startup Link Style ■ Default Link Bundle State ■ Tile Direction ■ Threshold Percent ■ Threshold Trigger Period <p>For more information on these defaults, see “Topology Options” on page 209.</p>
Log Parameters	<p>Lets you configure the log level as one of the following:</p> <ul style="list-style-type: none"> ■ Debug ■ Warning ■ Error ■ Info ■ Off ■ Fatal

Table 43: Options Categories (Continued)

Category	Description
File Transfer	<p>Lets you configure the following:</p> <ul style="list-style-type: none"> ■ Remote Host IP ■ Remote User Name ■ Remote Directory Path ■ Select Protocol ■ Password Required for FTP <p>For more information on these defaults, see “File Transfer Options” on page 210.</p>

Topology Options

Configure topology options to establish the default appearance of fabric topologies in Topology view. [Table 44](#) explains the default topology options that you can configure.

Table 44: Topology Options

Option	Description
Default Startup Layout pull-down menu	<p>Configures the topology layout that appears by default when you open Topology view. You can select from the following layouts:</p> <ul style="list-style-type: none"> ■ Circular layout arranges the switches and nodes of a fabric into a circle. ■ Core-Edge layout visually separates core switches, edge switches, and nodes. ■ Tree layout organizes the fabric hierarchically.
Default Startup Link Style pull-down menu	<p>Configures the link style that appears by default when you open Topology view. You can select from the following styles:</p> <ul style="list-style-type: none"> ■ Orthogonal style displays all links as horizontal and vertical lines that turn at right angles. ■ Straight style displays all links as straight, unbending lines that connect switches along the shortest path.
Default Link Bundle State pull-down menu	Designates the default link bundle state as expanded or collapsed.
Tile Direction pull-down menu	Designates the way you want non-connected graph objects to appear in relation to each other (horizontally or vertically).
Threshold Percent field	Configures the percent of bandwidth above which the link raises a flag.
Threshold Trigger Period field	<p>Configures the amount of time (in seconds) that the bandwidth of a link must exceed the threshold percent before the link raises a flag.</p> <p>You cannot configure this field to a value greater than 60 seconds.</p>
OK button	Applies configuration changes.
Cancel button	Aborts configuration changes.

File Transfer Options

Configure file transfer options to perform tasks such as firmware download that require FTP to execute. [Table 45](#) explains the file transfer options.

For instructions on configuring transfer options, see “[Configuring File Transfer Options](#)” on page 52.

Table 45: File Transfer Options

Option	Description
Remote Host IP field	Accepts the IP address of a host that runs FTP.
Remote User Name field	Accepts the user name with which to log in to the host.
Remote Directory Path field	Accepts the path on the server to access.
Select Protocol pull-down menu	Identifies the protocol to use to contact the host.
Password Required for FTP field	Accepts the password with which to log in to the host.
OK button	Applies file transfer changes.
Cancel button	Aborts file transfer changes.
Test button	Tests whether you can successfully access the host with the protocol you configured in the Select Protocol pull-down menu.
Help button	Opens Fabric Manager Help.

Edit Menu Reference



The **Edit** menu manages elements of the GUI. [Table 46](#) explains the options in the **Edit** menu.

Table 46: Edit Menu Options

Option	Description
Copy Table	<p>Copies a table so you can paste it into an application that uses tab-delimited cell/return-delimited row format.</p> <p>The Copy Table option is not available for the following views:</p> <ul style="list-style-type: none">■ Topology view■ Overview view■ LSAN view
Save Data	<p>Allows you to save a table as a tab-delimited file.</p> <p>The Save Data option is not available for the following views:</p> <ul style="list-style-type: none">■ Topology view■ Overview view■ LSAN view
Rename	<p>Changes the identifier of a switch, port, or fabric in the SAN Elements tab.</p> <p>This option does not reconfigure the Switch Name. It only changes how the fabric or switch appears in Fabric Manager.</p> <p>To select the Rename option, you must first click one of the following elements:</p> <ul style="list-style-type: none">■ A fabric in the SAN Elements tab■ A switch in the SAN Elements tab■ A port in the SAN Elements tab

Table 46: Edit Menu Options (Continued)

Option	Description
View options	Opens the Edit View Options for <i>X</i> window (where <i>X</i> represents the current active view) to customize the Fabric Manager display. For more information on this window, see “Edit View Options Windows” on page 212.
Sort order	Opens the Edit Sort Order dialog box, which allows you to sort the order of columns displayed in the table. This option is available only when you are in a view that displays information in table format.
Change description	<p>Opens the Please enter the new description dialog box to change the description of a pane. Every Fabric Manager view that displays a pane (for instance, Summary view when you click Fabrics in the San Elements tab) includes a description. By default, this description reads <code>Double click to add description</code>. This option provides an alternative method to change the description.</p> <p>After you change the description of an element, you must click the parent element to view the new description in the pane.</p>

Edit View Options Windows

You can customize view options in Fabric Manager. For more information about what information is available per view, see [Appendix C](#). For more information on how to customize views, see [“Device Ports Screen”](#) on page 44.

View Menu Reference



This appendix consists of the following sections:

- [“Introduction”](#) on page 214
- [“Overview View”](#) on page 215
- [“Alerts View”](#) on page 217
- [“Topology View”](#) on page 218
- [“Switches View”](#) on page 219
- [“Ports View”](#) on page 220
- [“Device Ports View”](#) on page 221
- [“Devices View”](#) on page 223
- [“Portgrid View”](#) on page 223
- [“LSAN View”](#) on page 223
- [“LSAN Info View”](#) on page 224

Introduction

The **View** menu lists the various Fabric Manager views. The sections that follow describe each view. You can use the **View** menu to navigate Fabric Manager just as you use the view selector.

Certain views in Fabric Manager are available only when you have particular element types selected from the **SAN Elements** tab. [Table 47](#) identifies which views are available at which element level.

Table 47: Selection of Views Available at Various Levels of SAN Hierarchy

	SAN	Fabric Node	Fabric	Switch	Card	Port	Switch Groups Node	Switch Group	Port Groups Node	Port Group
Overview View			X					X		
Alerts View			X	X				X		
Topology View			X	X	X	X		X		X
Events View			X	X	X	X		X		X
Ports View			X							
Switches View				X ¹						
Port Grid View			X					X		
Devices View			X	X				X		
Device Ports View			X	X	X	X		X		X
LSAN View			X	X	X	X		X		X
LSAN Info View			X							

1. The LSAN Info view is available only when you have an MP Router selected in the **SAN Elements** tab.

Table-Format View Buttons

The following Fabric Manager views display information in table format:

- Alerts view
- Events view
- Ports view
- Switches view
- Port Grid view

- Devices view
- Device Ports view
- LSAN view
- LSAN Info view

These table-format views can be copied, saved, and customized. [Table 48](#) describes the buttons.

Table 48: Table-Format View Buttons

Button	Description
Copy table	Click Copy Table to copy the information displayed in the selected view to the clipboard.
Save data	Click Save Data to open the data to a tab-delimited file dialog box, where you can save the information displayed in the selected view to a tab-delimited file and open in it an external application.
View options	Click View Options to open the Edit View Options dialog box, where you can customize the information displayed in the selected view.
Sort order	Click Sort Order to open the Edit Sort Order dialog box, where you can customize the order of the information, as well as the order of the columns, displayed in the selected view.


Overview View

The Overview view displays a graphical overview of the child elements to the element selected in the **SAN Elements** tab. For example, if you have the fabric selected in the **SAN Elements** tab, all switches within that fabric are displayed in the Overview view. Each switch has its own At-A-Glance window, and information about the switch as well as a switch icon is displayed in the window. You can customize the information that is displayed about each element in its At-A-Glance window in the Overview view. To customize the view options for an element, see “[Device Ports Screen](#)” on page 44.

Each At-A-Glance window includes a series of icons at the bottom. The icons in the bottom-left corner of each pane represent the element type. One icon is displayed for each type of element that is under that node.

When you select the **SAN** node from the **SAN Elements** tab, certain icons are displayed in the bottom-right corner of each node At-A-Glance window. [Table 49](#) describes the icons.








Table 49: SAN Node Icons

Icon	Description
Edit View Options icon	Opens the Edit View Options dialog box so you can customize the information displayed in the view.
Update icon 	Updates the information in the display pane.

Fabric At-A-Glance Windows

Table 50 describes the icons displayed in each fabric At-A-Glance window when you select the **Fabrics** node from the **SAN Elements** tab.







Table 50: Fabrics Node Icons

Icon	Description
Fabric Events icon 	Opens Event view in a new Fabric Manager window for the appropriate fabric. (For instance, if you click the Events icon in the Switch X pane, Fabric Manager selects Switch X from the SAN Elements tab and opens Event view.) For more information, see “ LSAN Info View ” on page 224.
Zone Admin icon 	Opens the Zone Admin windows of Advanced Web Tools.
Name Server icon 	Opens the Name Server Table window of Advanced Web Tools.
Fabric Topology icon 	Opens Advanced Web Tools topology view to show tables of data that display the routes that the data takes.
Security Admin con 	Opens the Security Admin window. For more information, see Chapter 10 . This icon appears only in the pane of a secure fabric.
Telnet to FCS icon 	Opens a Telnet session to the FCS. For more information, see Chapter 10 . This icon appears only in the pane of a secure fabric.
Update icon 	Updates the information in the display pane.

Switch At-A-Glance Windows

Table 51 describes the icons displayed in each switch At-A-Glance window when you select a particular fabric from the **SAN Elements** tab.

Table 51: Switch At-A-Glance Icons

Icon	Description
Switch Events icon 	Opens Event view for the switch in a new Fabric Manager window.
Admin View icon 	Opens the Switch Admin window of Advanced Web Tools.
Fabric Watch icon 	Opens the Fabric Watch window of Advanced Web Tools.
Health Report icon 	Opens the switch health report. The switch health report is available only for switches running firmware versions later than Fabric OS v4.2.0x. For switches running 4.2.0x or earlier, the switch health report is unavailable and the icon is not displayed in the At-A-Glance view for that switch.
Telnet icon 	Opens a Telnet session to the switch.
Update icon 	Updates the information in the display pane.

Port At-A-Glance Windows

Table 52 describes the icon displayed in the port At-A-Glance window when you select a switch from the **SAN Elements** tab.





Table 52: Port At-A-Glance Switch Detail Icon

Icon	Description
Update icon 	Updates the information in the display pane.

SwitchGroups At-A-Glance Windows

Table 53 describes the icons displayed in each switchgroup At-A-Glance window when you select the **Switchgroups** node from the **SAN Elements** tab.




Table 53: SwitchGroups Detail Icons

Icon	Description
Group Events icon 	Opens Event view for the switch in a new Fabric Manager window.
Group Creation icon 	Opens the Edit Switch Group window. For more information on this window, see “ Edit Switch Groups Window ” on page 207.
Group Exportation icon 	Opens the Export window.
Update icon 	Updates the information in the display pane.

PortGroups At-A-Glance Windows

Table 54 describes the icons displayed in each portgroup At-A-Glance window when you select the **Portgroups** node from the **SAN Elements** tab.

Table 54: PortGroups Detail Icons

Icon	Description
Group Creation icon 	Opens the Edit Port Group window. For more information on this window, see “ Edit Port Groups Window ” on page 208.
Group Exportation icon 	Opens the Export window.
Update icon 	Updates the information in the display pane.

Alerts View

The Alerts view displays all alerts that you configure to be generated by Fabric Manager. Switch status, switch unreachable, and Change Management triggered alerts are displayed in the Alerts view (see Table 55).

You can customize the information that is displayed in the Alerts view. To customize the view options, see “[Device Ports Screen](#)” on page 44.

Table 55: Alerts View Display

Column	Description
#	Row number; this column makes it easier to sort table information.
First Occurrence	Identifies the time of the first occurrence of the alert.
Last Occurrence	Identifies the time of the last occurrence of the alert.
Description	Describes the alert type.
Severity	Identifies the alert severity.
Source	Identifies the source of the alert.
Ack Status	Indicates the acknowledgement status of the alert.
Acknowledger	Identifies the user ID of the user who acknowledged the alert.
Ack Time	Identifies the time the alert was acknowledged.
Resolve Status	Identifies the resolution status of the alert.
Resolve Time	Identifies the time the alert was resolved.

Topology View

Topology view provides a graphical representation of the elements that Fabric Manager monitors and the connections among them. When you display Topology view, a number of icons appear at the top of the Fabric Manager window. [Table 56](#) describes these icons.

Note: Topology view may take a considerable amount of time to open. Topology view options may also respond slowly.

Table 56: Topology View Icons











Icon	Description
Pan icon 	Lets you click and drag the Topology view to pan up, down, left, & right to see different portions of the view.
Select icon 	Lets you move nodes in Topology view.
Zoom in rect icon 	Lets you click and drag to zoom in on a particular rectangular region of the topology.
Zoom in icon 	Click to zoom in.
Zoom out icon 	Click to zoom out.
Fit to view icon 	Click to fit the entire topology in your Fabric Manager window.
Overview icon 	Opens a new window that displays the entire topology in miniature.

Table 56: Topology View Icons (Continued)

Icon	Description
Snap Shot icon 	Takes a screen shot of your topology graph that you can save in .png format.
Straight Link Style icon 	Arranges links so they connect in a straight line from one element to another.
Orthogonal Link Style icon 	Arranges links in horizontal and vertical lines, with right angles, to connect elements.

Each Topology view consists of nested panes and element icons. Element icons that contain other elements (for instance, as a fabric contains switches) include an expand (+) icon in the top left corner. If you expand the icon, the icon becomes a pane that displays the nested icons. Panes include a collapse icon (-) in the top left corner so you can hide the subordinate icons.

Switches View

Table 57 describes the information that the Switches view displays about switches.

Table 57: Switches View Display

Property	Description
Name	Displays the name of the switch.
IP	Displays the IP address of the switch.
Version	Displays the firmware version that the switch runs.
Status	Displays the status of the switch.
Fabric	Displays the fabric to which the switch connects.
ID	Displays the ID that you choose from the ID pull-down menu. For more, see “Displaying SAN Elements by IP address, Domain ID, WWN, and Name” on page 50.
IP Mask	Displays the subnet mask of the switch.
Gateway	Displays the gateway of the switch.
FCIP	Displays the FC IP address of the switch, if configured.
FC Mask	Displays the FC mask of the switch, if configured.
Responding	Displays true if the switch responds to Fabric Manager and false if it does not.
Role	Displays the role that the switch plays in the fabric (principal or subordinate).
Domain ID	Displays the domain ID of the switch.
WWN	Displays the WWN of the switch.
State	Displays whether the switch is enabled or disabled.
Is Core	Displays whether the switch is a core switch or an edge switch. For more information, see “Designating a Switch as a Core Switch” on page 54.
Port Count	Displays the number of ports in the switch.
Free Ports	Displays the number of unused/available ports in the switch.
ISL Count	Displays the number of ISLs (E_Ports) connected to the switch.
Secure Mode	Displays whether Secure Mode is enabled or disabled.
Using FCIP	Identifies whether or not the switch is configured for FCIP.

Table 57: Switches View Display (Continued)

Property	Description
Have UserID	Identifies whether or not user information has been added to a switch. Provides fabric login (flogi) status.
Has Certificate	Identifies whether or not a security certificate is installed.
Trunk Count	Displays the number of trunks that connect to the switch.
Trunked Port Count	Displays the number of ports in each trunk that connects to the switch.
Device Count	Displays the number of devices that connect to the switch.
IDID	Identifies whether Insistent Domain ID Mode (IDID Mode) is enabled or disabled; a value of <code>true</code> indicates it is enabled; a value of <code>false</code> indicates it is disabled.
Type Number	Displays a string that represents switch type. These values come from the switch RNID database.
Model	Displays the switch model number.
Manufacturer	Displays the switch manufacturer.
Plant of Manufacture	Displays the plant of manufacture.
Type	Displays the switch type.
Switch Part Number	Identifies the chassis part number, for applicable switches.
Serial Number	Identifies the switch serial number.
Supplier Serial Number	Displays the supplier serial number.

Ports View

Ports view provides detailed information on every port in the switch you select from the **SAN Elements** tab. The view includes status information. The following events (and only these events) change the port status to down:

- Diag_Flt
- Lock_Ref
- Port_Flt
- No_Sync
- Laser_Flt
- No_Port

The following events (and only these events) change the port status to marginal:

- No_Light
- Disabled
- Testing

The following events (and only these events) change the port status to healthy:

- In_Sync
- No_Module
- No_Card
- Online

[Table 58](#) describes the details that appear in Ports view.

Table 58: Ports View Display

Property	Description
#	Row number; this column makes it easier to sort table information.
Fabric	Displays the name of the fabric to which the port belongs.
Switch	Displays the name of the switch to which the port belongs.
ID	Displays the port ID of the port.
Status	Displays the status of the port. The background color of the status fields also change to reflect the port status visually.
Responding	Indicates the current responding state of the HTTP session.
State	Displays the state of the port module.
Type	Displays the port type of the port.
Speed	Displays the speed of the port in Gbps.
Port Module	Displays whether the port is copper or fiber.
Card Number	Identifies the card in a dual-switch chassis to which the port belongs.
Port Number	Displays the number of the port in the port card (0-15).
User Port Number	Displays the number of the port in the switch (variable).
Area ID	Displays the area ID of the port.
WWN	Displays the WWN of the port.
Name	Displays the name that you assigned to the switch with Fabric Manager. For more information, see “Renaming a Port” on page 43.

Device Ports View

The Device Ports view lists the device ports attached to a given element in the **SAN Elements** tab. The properties that the Device Ports view displays appear in [Table 59](#).

Table 59: Device Ports View Display

Column	Description
Domain ID	Identifies the domain ID.
Port	Identifies the device and the port on that device.
Port ID	Identifies the port ID, in hexadecimal format.
Port Type	Identifies the port type.
Fabric Port WWN	Identifies the fabric port world wide name.
Device Port WWN	Identifies the device port world wide name.

Table 59: Device Ports View Display (Continued)

Column	Description
Device Node WWN	Identifies the device node world wide name.
Device Name	Identifies the device name.
Physical/Virtual	Identifies the device port as physical or virtual.
Role	Identifies the role as target, initiator, both, or unknown. In the Device Ports view, the Role column displays information only for switches running firmware versions later than 4.2.0x. If you have a switch or director running firmware versions 4.2.0x or earlier, the value for the Role column in the Device Ports view is displayed as <code>Unknown</code> .
FC4 Type	Identifies the FC4 type.
COS	Identifies the class of service.
Port IP Address	Identifies the port IP address.
Hard Address	Identifies the hard address.
Manufacturer	Identifies the device's manufacturer.
Sequence Number	Identifies the sequence number.
Device Type Number	Identifies the device type number.
Model	Identifies the model number.
Manufacturing Plant	Identifies the manufacturing plant of the device.
Tag	Identifies the device tag.
Capability	Identifies the device capability.

Devices View

Devices view lists the devices attached to a given element in the **SAN Elements** tab. [Table 60](#) lists the properties displayed in the Devices view.

Table 60: Devices View Display

Column	Description
Device Node WWN	Displays the world wide name of the device.
SCSI Inquiry Name	Displays the SCSI inquiry name of the device. The SCSI inquiry name serves as the symbolic SCSI name of the device. If the device does not have a SCSI inquiry name, nothing appears in this field.
Physical/Virtual	Identifies the device as physical or virtual.
Role	Identifies the role as target, initiator, both, or unknown. In the Devices view, the Role column displays information only for switches running firmware versions later than 4.2.0x. If you have a switch or director running firmware versions 4.2.0x or earlier, the value for the Role column in the Devices view is displayed as <i>Unknown</i> .
Serial number	Displays the serial number of FDMI-capable HBAs.
Model Description	Displays a description of an FDMI-capable device.
Hardware	Displays an internal identifier of the FDMI-capable HBA manufacturer.
Driver	Displays the driver that host runs for that HBA.
ROM version	Indicates the ROM version.
Firmware	Displays the firmware that the HBA runs.
OS name and version	Displays the OS of the device on which the HBA is installed.

Portgrid View

Portgrid view displays which ports connect to which devices for switches. Portgrid view works only when you click **My SAN**, **Fabrics**, or a specific fabric or switch in the **SAN Elements** tab. If a device has a SCSI Inquiry Name, Portgrid view displays it. If not, Portgrid view displays the WWN. For loop devices, Portgrid view shows *loop* and the number of devices in the loop.

LSAN View

The LSAN view is displayed only when a fabric being monitored by Fabric Manager has an MP Router (see [Table 61](#)).

Table 61: LSAN View Display

Property	Description
#	Row number; this column makes it easier to sort table information.
Device Name	The device name.
Device Port WWN	The port WWN.
Fabric Name	The name of the fabric to which the LSAN belongs.
Fabric ID	The fabric ID to which the LSAN belongs.

Table 61: LSAN View Display (Continued)

Property	Description
Share Status	The share status as imported or exported.
Modify button	Click to modify the LSAN.
Delete button	Click to delete the selected LSAN.

LSAN Info View

The LSAN Info view is available only when you select an MP Router from the **SAN Elements** tab. It has three tabs: **Physical Device**, **Virtual Devices**, and **LSAN Information**.

Physical Devices Tab

The **Physical Devices** tab displays information about the physical devices attached to the router (see [Table 62](#)).

Table 62: LSAN View Physical Devices Tab

Property	Description
#	Row number; this column makes it easier to sort table information.
EX Ports	The ports to which the router is attached.
Fabric Name	The name of the fabric to which the physical devices belong.
Fabric ID	The fabric ID to which the physical devices belong.
Device Name	The devices name.
Device Port WWN	The device port WWN.
Device PID	The device port ID.
LSANs	The LSANs to which the physical devices belong.

Virtual Devices Tab

The **Virtual Devices** tab displays information about the virtual devices attached to the router (see [Table 63](#)).

Table 63: LSAN View Virtual Devices Tab

Property	Description
#	Row number; this column makes it easier to sort table information.
Fabric Name	The name of the fabric to which the virtual devices belong.
Fabric ID	The fabric ID to which the virtual devices belong.
Device Name	The devices name.
Device Port WWN	The device port WWN.
Device PID	The device port ID.
LSANs	The LSANs to which the virtual devices belong.

LSAN Information Tab

The **LSAN Information** tab displays information about the selected LSAN (see [Table 64](#)).

Table 64: LSAN View LSAN Information Tab

Property	Description
#	Row number; this column makes it easier to sort table information.
Fabric Name	The name of the fabric to which the LSAN belongs.
Fabric ID	The fabric ID to which the LSAN belongs.
LSAN Name	The LSAN name.
LSAN Member Name	The LSAN member name.
Member Port WWN	The member port WWN.

Actions Menu Reference



This appendix consists of the following sections:

- [“Introduction”](#) on page 227
- [“Fabric Actions”](#) on page 227
- [“Switch Actions”](#) on page 230
- [“Port Actions”](#) on page 230

Introduction

The **Actions** menu displays tasks that you can perform with Fabric Manager. You can access items in this menu only in the following cases:

- When you click a specific fabric in the **SAN Elements** tab
- When you click a specific switch in the **SAN Elements** tab
- When you click a switchgroup node in the **SAN Elements** tab
- When you click a switchgroup in the **SAN Elements** tab
- When you click a specific port in the **SAN Elements** tab
- When you click a portgroup node in the **SAN Elements** tab
- When you click a portgroup in the **SAN Elements** tab
- When you click a specific card in the **SAN Elements** tab (for switches that support cards)

Fabric Actions

When you click a fabric in the **SAN Elements** tab and open the **Actions** menu, the menu provides a series of fabric-wide tasks that you can perform. [Table 65](#) describes the actions.

Table 65: Fabric Actions

Action	Description
Events	Opens the Events View.
Telnet to FCS	Telnets to the FCS of a secure fabric. If you click a non-secure fabric in the SAN Elements tab, you cannot access this action and it appears as Telnet. This option appears only when you click a secure fabric in the SAN Elements tab.
Telnet	Opens a Telnet window. This option is available only from non-secure fabrics in the SAN Elements tab.
MP Router Configuration	Opens the FC Router configuration module. For more information, see Chapter 18, “Using Fabric Manager With the MP Router.”
Security	Allows you to enable or disable security on a fabric, manage security policies, and merge secure fabrics.
Zone Admin	Opens the Zone Administration window of Advanced Web Tools. For more information, see Chapter 21, “Using the Zoning Module in Fabric Manager.”
Name Server	Opens the Name Server Table window in Advanced Web Tools. For more information, see Chapter 7, “Name Server.”
Set Time	Opens the Time dialog box to update the time and date settings on the switches in the fabric. To configure the time, place your cursor in any part of the Time field, use the up arrow and down arrows to iterate the field, and then click OK .
Refresh FDMI Info	Refreshes FDMI information. This option appears only when FDMI-capable HBAs are connected to switches running Fabric OS versions that support FDMI.
Performance Monitoring	Allows you to turn port history recording on or off, and when it is on, you can create custom reports, generate reports from templates, or access saved reports.
Delete	Deletes the selected fabric.
Rename	Allows you to rename the selected fabric.

Security Admin Window

The Security Admin window consists of tabs that let you view and configure the various security policies. [Table 66](#) describes the tabs and buttons in the Security Admin window.

Table 66: Security Admin Window Objects

Object	Description
Summary tab	Presents a column of defined security policies and a column of active security policies.
SCC tab	The components of this tab let you add a switch to a secure fabric. For more information, see “Configuring SCC Policy Options” on page 154.
FCS tab	The components of this tab display each switch that serves as a Fabric Configuration Server (FCS) and lets you add or remove switches from the list. For more information, see “Configuring FCS Policy Options” on page 152.
TELNET tab	The components of this tab allow the host to access the fabric using the Telnet protocol. For more information, see “Configuring Telnet, RSNMP, WSNMP, HTTP, and API Policy Options” on page 155.

Table 66: Security Admin Window Objects (Continued)

Object	Description
RSNMP tab	The components of this tab let you grant access to individual switches to run RSNMP (read-only SNMP) in a secure fabric. For more information, see “Configuring Telnet, RSNMP, WSNMP, HTTP, and API Policy Options” on page 155.
WSNMP tab	The components of this tab let you grant access to individual switches to run WSNMP (read/write SNMP) in a secure fabric. For more information, see “Configuring Telnet, RSNMP, WSNMP, HTTP, and API Policy Options” on page 155.
HTTP tab	The components of this tab allow a host HTTP access into the fabric. For more information, see “Configuring Telnet, RSNMP, WSNMP, HTTP, and API Policy Options” on page 155.
API tab	The components of this tab allows hosts to access the fabric using the HP API. For more information, see “Configuring Telnet, RSNMP, WSNMP, HTTP, and API Policy Options” on page 155.
DCC tab	The components of this tab let you create a security policy to bind device ports to switch ports. For more information, see “Configuring DCC Policy Options” on page 160.
MS tab	The components of this tab let you grant access to individual switches to run Management Server in a secure fabric. For more information, see “Configuring MS Policy Options” on page 161.
SERIAL tab	The components of this tab let you grant access to individual switches to accept a serial connection in a secure fabric. For more information, see “Configuring Serial and Front Panel Policy Options” on page 162.
FRONTPANEL tab	The components of this tab let you grant access to individual switches to accept configuration changes from the front panel in a secure fabric. For more information, see “Configuring Serial and Front Panel Policy Options” on page 162.
Options tab	The field in this tab lets you enable or disable No Node WWN zoning.
Password tab	The components of this tab let you change passwords for FCS switches and non-FCS switches.
Activate button	Activates the changes that you made to the components of the Security Admin window tabs.
Save button	Saves the changes that you made to the components of the Security Admin window tabs but does not apply them.
Close button	Closes the Security Admin window.

Switch Actions

When you click a switch in the **SAN Elements** tab and open the **Actions** menu, the menu provides a series of switch-wide tasks that you can perform. [Table 67](#) describes the actions.

Table 67: Switch Actions

Action	Description
Switch View	Opens the Switch View window of Advanced Web Tools.
Events	Opens the Events View in Fabric Manager.
Admin	Opens the Switch Admin window of Advanced Web Tools.
Fabric Watch	Opens the Fabric Watch window of Advanced Web Tools.
Health Report	Opens the Switch Health Report. The switch health report is available only for switches running firmware versions later than Fabric OS v4.2.0x. For switches running 4.2.0x or earlier, the switch health report is unavailable and the icon is not displayed in the At-A-Glance view for that switch.
Firmware Download	Opens the Firmware Download dialog box.
Telnet	Opens a Telnet session to the switch.
Close Telnet	Closes a Telnet session to the switch. This option is not applicable to switches that run 4x firmware.
Supportshow	Allows you to save <code>supportshow</code> command information to a file.
Port Address Configuration	Allows you to select port connectivity configurations (active or stored).
Disable/Enable	Disables or enables the switch.
Core Switch	Labels a switch as a core switch. This action impacts the location of the switch in Topology view for Core Edge layouts.
Delete	Deletes the switch from Fabric Manager.
Rename	Renames the Switch in Fabric Manager.

Port Actions

When you click a port in the **SAN Elements** tab and open the **Actions** menu, the menu provides port-wide tasks that you can perform. [Table 68](#) describes the actions.

Table 68: Port Actions

Action	Description
Disable/Enable	Disables or enables the port.
Delete	Deletes the port from Fabric Manager.
Rename	Renames the port in Fabric Manager.

Topology Menu Reference



The **Topology** menu provides options to help you use and customize Topology view. You can access the **Topology** menu only after you open Topology view. [Table 69](#) describes **Topology** menu options.

Fabric size impacts Topology view response speed.

Table 69: Topology Menu Options

Option	Description
Layout	Opens the Layout submenu to select a layout or clear any changes you made to the layout. The layout options are as follows: <ul style="list-style-type: none">■ Circular: Arranges the switches and nodes of a fabric into a circle.■ Core-Edge: Separates core switches, edge switches, and nodes.■ Tree: Organizes the fabric hierarchically. For more information on Topology view layouts, see “Topology View” on page 218.
Links	Opens the Links submenu to: <ul style="list-style-type: none">■ Expand all links■ Collapse all links■ Orthogonal link style■ Straight link style
Overview	Opens a new window that displays the entire topology in miniature.
Snapshot	Takes a snapshot of your current topology so you can compare a later topology to this baseline.

Tools Menu Reference



This appendix consists of the following sections:

- [“Introduction”](#) on page 233
- [“Reboot Submenu”](#) on page 234
- [“Config Submenu”](#) on page 234
- [“Licensing Submenu”](#) on page 235
- [“Change Management Submenu”](#) on page 235

Introduction

The **Tools** menu serves as a toolbox of mini-applications to help you perform a variety of tasks. [Table 70](#) describes the options in the **Tools** menu.

Table 70: Tools Menu Options

Option	Description
Firmware download to switches	Opens the Firmware download to switches window. For more information on how to download firmware to switches with Fabric Manager, see Chapter 12, “Downloading Firmware.”
Firmware download to HBAs	Opens the Firmware download to HBAs window. For more information on how to download firmware to HBAs with Fabric Manager, see Chapter 19, “FDMI-Capable HBA Firmware Download.”
Reboot	Opens the Reboot submenu to configure or execute a sequenced reboot. For more information, see “Reboot Submenu” on page 234.
Config	Opens the Config submenu to save a baseline configuration or to compare configurations. For more information, see “Config Submenu” on page 234.
Licensing	Opens the Licensing submenu to manage software licenses. For more information, see “Licensing Submenu” on page 235.
Change Management	Opens the Change Management wizard to manage how changes are handled in your fabric. For more information, see Chapter 6, “Change Management.”
Fabric Merge	Opens the Fabric Merge Check dialog box to verify that you can merge two fabrics successfully. For more information, see “Comparing Fabrics for a Fabric Merge” on page 100.
Subnet scan	Opens the Subnet scan dialog box to discover available fabrics. For more information, see “Running a Subnet Scan (Fabric Scan)” on page 41.

Table 70: Tools Menu Options (Continued)

Option	Description
Call Home	Opens the Call Home window. For more information, see Chapter 16, "Call Home."
Notification Configuration	Opens the Notification Config dialog box, where you can configure notification parameters for Change Management mail notifications and the Call Home email notifications on a global basis. For more information, see "Configuring Notification Parameters" on page 71.
Share Devices	Opens the Share Devices wizard, where you can set up shared devices easily. For more information, see "Sharing Devices Between Fabrics" on page 142.

Reboot Submenu

The **Reboot** submenu helps you prepare and execute a sequenced reboot. [Table 71](#) describes the options in this menu.

Table 71: Reboot Submenu Options

Option	Description
Create Reboot Sequence	Opens the Create or change reboot groups and sequence window to make or edit a reboot group. For more information on how to create and change reboot groups, see Chapter 13, "Tools Menu Reference."
Sequence Reboot	Opens the Sequenced Reboot window to execute a sequenced reboot. For more information, see Chapter 13, "Tools Menu Reference."

Config Submenu

The **Config** submenu provides options that let you save, download, and compare configuration files. [Table 72](#) describes the options in this menu.

Table 72: Config Submenu Options

Option	Description
Save Baseline	Opens the Save Baseline -- Configuration Template Selection dialog box so you can begin to save the configuration file of a switch to a server. For more information about how to save a baseline, see "Saving a Baseline Configuration to a File" on page 90.
Compare/Download From File	Opens the Compare/Download from File -- Select Baseline Configuration window to choose a file to compare or download. For more information on comparing and downloading configurations, see Chapter 9, "Comparing Configurations."
Compare/Download From Switch	Opens the Compare/Download from Switch -- Source Configuration Selection window to select a switch so you can compare to the configuration of that switch or download the configuration of that switch. For more information on comparing and downloading configurations, see Chapter 9, "Comparing Configurations."

Licensing Submenu

The **Licensing** submenu provides options that let you manage licenses with Fabric Manager. [Table 73](#) describes the options in this menu.

Table 73: Licensing Submenu Options

Option	Description
Import from File	Opens the Import License -- Select license file dialog box to import license keys from a file that you can apply to one or more switches. For more information on how to import a license file, see "Exporting and Importing License Keys" on page 102.
Load from Switch	Opens the License Admin -- Switch Selection window. For more information on how to load licenses from a switch, see Chapter 6, "Change Management."
Generate Licenses	Opens the Create License Request -- Select transaction key file or saved request window to obtain licenses and later apply them to switches.
Load Generated Licenses	Opens the License Admin -- Switch Selection window to open previously-saved license files which you can then download to switches.

Change Management Submenu

The **Change Management** submenu provides options that allow you to configure how fabric changes are managed in Fabric Manager. For more information on change management, see [Chapter 6 "Change Management."](#) [Table 74](#) describes the options in the submenu.

Table 74: Change Management Submenu

Option	Description
Manage Profiles	Allows you to manage the change management profiles you created. For more information, see "Displaying Saved CM Profiles" on page 73.
View Change Reports	Allows you to view the change reports. For more information, see "Displaying a Change Report" on page 75.

Help Menu Reference



The **Help** menu provides access to information about Fabric Manager. [Table 75](#) describes the options that appear in the **Help** menu.

Table 75: Help Menu Options

Option	Description
Help	Opens Fabric Manager Online Help.
Context Help	Creates a pointer to provide help about the portion of Fabric Manager that you click.
Status Legend	Displays the Fabric Manager status legend.
Register	Opens Fabric Manager Registration dialog box. For details, see “Registering Fabric Manager” on page 40.
About	Provides information about your version of Fabric Manager.

index

A

- actions menu 185, 227 to 230
- address field 22
- alarms
 - configuring 61
 - enabling and disabling 63
 - notification tab 64
 - viewing 61
- alerts
 - acknowledging 119
 - change management triggered 118
 - deleting 119
 - fabric manager 117 to 119
 - identifying switches and fabrics with 118
 - resolving 119
 - switch status change 117
 - switch unreachable 117
 - view 217
- alias tab 185
- alias, defined 168
- at-a-glance windows 24
- audience 15
- authentication
 - fabric manager 33
 - failure of 126
 - issues with 196
 - NIS 35, 197
 - password file 35
 - Windows domain 196
- authorized reseller, HP 17

B

- baseline configuration, saving to a file 90
- baseline templates, customizing 93

C

- call home 121 to 124
 - configuration wizard 122
 - configuring 122

- editing configuration 124
- enabling and disabling 124
- change management
 - creating a profile 71
 - creating snapshots 76
 - deleting profiles 73
 - feature 69
 - profiles 70
 - submenu 235
 - triggered alerts 118
 - wizard 71, 233
- change reports
 - displaying 75, 76
 - printing 77
- client, fabric manager 28
- clone profile wizard 74
- commands
 - configure 90
 - dxdiag 202
 - fabricshow 109, 200
 - SCSI inquiry 80
 - supportshow 20, 121, 201, 230
- comparing configurations, best practices 90
- config submenu 234
- config tab 192
- configurations
 - defined 168
 - downloading 51
- configure command 90
- configuring
 - alarms 61
 - API policy options 159
 - call home 122
 - DCC policy options 160
 - email alert recipient 62
 - FCS policy options 152
 - file transfer options 52
 - front panel policy options 162
 - HTTP policy options 158
 - no node WWN zoning 164

- notification parameters 71
- RSNMP policy options 157
- SCC policy options 154
- security policy options for 152
- serial policy options 162
- threshold behavior 63
- topology view options 86
- WSNMP policy options 157
- conventions
 - document 16
 - text symbols 16
- core switch, assigning manually 85
- create secure fabric wizard 150
- creating
 - configuration analysis report 182
 - fabric assist zone 180
 - port groups 114
 - quickloops 178
 - reboot groups 110
 - secure fabrics 150
 - single switch reboot groups 111
 - switch groups 114
 - templates 97
 - zone configuration 169
 - zones 177
- customizing baseline templates 93
- customizing views 45

D

- database name server 79
- databases
 - fabric manager 20, 71, 117
 - simple name server 79
 - zoning 100, 170
- deleting
 - alerts 119
 - fabric assist zones 181
 - fabrics 42
 - quickloops 179
 - zone configurations 182
 - zones 178
- device ports view 221
- devices view 223
- disabling
 - alarms 63
 - performance monitoring 128
 - zone configuration 174
- discovered fabric topologies, viewing 86
- discovering a fabric 41
- displaying
 - change reports 75, 76
 - LSANs 144
 - name server entries 81
 - XML reports 139

- zone configuration 171
- zone members 81
- document conventions 16
- documents, related 15
- domain names, valid 35
- downloading configurations 51
- downloading firmware to an HBA 145
- dxdiag command 202

E

- edge fabrics, connecting 143
- edit menu 184, 211 to 212
- edit port groups window 208
- edit switch groups window 207
- edit view options window 212
- editing
 - call home configuration 124
 - performance monitor graphs 138
 - templates 97
- e-licensing 103
- enabling
 - alarms 63
 - performance monitoring 128
 - zone configuration 173
- environments
 - Solaris 28
 - windows 27
- evaluation version 32
- event log table fields 58
- exporting snapshots 76

F

- fabric assist tab 190
- fabric at-a-glance window 216
- fabric events, viewing and refreshing 57
- fabric login window 206
- fabric manager
 - alerts 117 to 119
 - authentication 33
 - changed features 20
 - checking 196
 - client 28
 - database 20, 71, 117
 - evaluation version 32
 - full version 32
 - icons 22
 - installing client and server 33
 - installing client only 36
 - launching 39
 - new features 19
 - registering 40
 - server 29
 - uninstalling 40

- upgrading 37
- views 25
- fabric merge, comparing fabrics 100
- fabric watch
 - alarm configuration report 64
 - dialog box reference 64
 - launching 61
 - terms and definitions 60
 - using 60
- fabrics
 - adding switches to 166
 - connecting 143
 - creating secure 150
 - deleting 42
 - discovering 41
 - merging secure 166
 - refreshing 173
 - renaming 42
 - sharing devices between 142
 - synchronizing time and date 53
- fabricshow command 109, 200
- fabric-wide tasks 227
- fields
 - address 22
 - event log table 58
- file menu 183, 205 to 210
- file transfer options 210
- file transfer options, configuring 52
- file transfer protocol 52
- files
 - HTML 76
 - license request 103
 - password 35
 - persistent 26
 - property 38
 - readme 35
 - systeminfo 39
 - template 94
 - transaction key 103
 - XML 76, 94
- filter tab 26
- firmware
 - controlling download reboots 107
 - downloading 105 to 107
 - downloading to an HBA 145
 - downloading to multiple switches 106

G

- generating custom graphs and reports 129
- getting help 17
- granularity
 - of reports 125
 - options 126
- graphs

- editing 138
- generating custom 129
- generating from templates 138
- groups submenu 207

H

- help menu 237
- help, obtaining 17
- HP
 - authorized reseller 17
 - storage website 17
 - technical support 17
- HTML file 76
- HTTP protocol 27

I

- icons, standard fabric manager 22
- ID menu 25
- installation wizard 34, 202
- installing
 - client and server 33
 - client only 36

L

- launching
 - fabric manager 39
 - fabric watch 61
 - policy editor 152
- license keys
 - importing and exporting 102
 - removing from a switch 102
- license request file 103
- licenses, obtaining 103
- licensing 101 to 104
- licensing submenu 235
- links in topology view 84
- log level, setting 50
- LSAN
 - displaying 144
 - info view 224
 - information tab 225
 - view 223

M

- menus
 - actions 185, 227 to 230
 - edit 184, 211 to 212
 - file 183, 205 to 210
 - help 237
 - ID 25
 - tools 233 to 235
 - topology 231
 - view 184, 213 to 225

merge secure fabrics wizard [166](#)
merging secure fabrics [166](#)

N

name server
 database [79](#)
 displaying entries [81](#)
 table entries [80](#)
NIS authentication [35](#), [197](#)
notification parameters, configuring [71](#)

O

operating systems supported [28](#)
options
 file transfer [210](#)
 topology [209](#)
 window [208](#)
overview view [215](#)

P

password file [35](#)
password file authentication [35](#)
performance monitoring [125](#) to [140](#)
 enabling and disabling [128](#)
persistent files [26](#)
physical devices tab [224](#)
policy editor, launching [152](#)
policy options, configuring
 API [159](#)
 DCC [160](#)
 FCS [152](#)
 front panel [162](#)
 HTTP [158](#)
 RSNMP [157](#)
 SCC [154](#)
 serial [162](#)
 WSNMP [157](#)
port at-a-glance window [217](#)
port groups
 creating [114](#)
 deleting [115](#)
 editing [115](#)
portgrid view [223](#)
portgroups at-a-glance window [217](#)
ports view [220](#)
ports, renaming [43](#)
port-wide tasks [230](#)
prefix tag [96](#)
printing
 change reports [77](#)
 snapshots [77](#)
 view information [47](#)
profiles

 creating a change management [71](#)
 deleting [73](#)
 displaying a saved [73](#)
 duplicating [74](#)
 editing [74](#)
property file [38](#)

Q

quickloop tab [189](#)
quickloops
 creating [178](#)
 deleting [179](#)
 modifying members of [179](#)
 renaming [180](#)

R

readme file [35](#)
reboot groups
 assigning switches to [111](#)
 creating [110](#)
 creating single switch [111](#)
reboot submenu [234](#)
reboots
 controlling firmware download [107](#)
 options [109](#)
 performing a sequenced [112](#)
 sequenced [109](#) to [112](#)
refreshing fabric events [57](#)
registering fabric manager [40](#)
related documentation [15](#)
renaming
 fabric assist zones [181](#)
 fabrics [42](#)
 ports [43](#)
 quickloops [180](#)
 switches [43](#)
 zone aliases [176](#)
 zone configurations [182](#)
 zones [178](#)
reports
 changing [77](#)
 displaying XML [139](#)
 generating custom [129](#)
 granularity of [125](#)
 snapshot [70](#)
 templates for [127](#)
requirements, system [27](#)

S

SAN element groups [113](#)
SAN elements tab [25](#)
SCSI inquiry command [80](#)
section tag [95](#)

- security 147 to 166
 - admin window 228
 - configuring policy options 152
 - levels 148
- sequenced reboots 109 to 112
- server, fabric manager 29
- share devices wizard 142, 234
- simple name server database 79
- simultaneous login 48
- snapshots
 - comparing 76
 - creating on demand 76
 - exporting 76
 - of topologies 87
 - printing 77
 - reports 70
- Solaris environments 28
- storing user settings 26
- submenus
 - change management 235
 - config 234
 - groups 207
 - licensing 235
 - reboot 234
- subnet scan, running 41
- supported operating systems 28
- supported upgrade paths 37
- supportshow command 20, 121, 201, 230
- switch at-a-glance window 216
- switch groups
 - creating 114
 - deleting 115
 - editing 115
- switch status change alerts 117
- switches
 - comparing to a baseline 91
 - renaming 43
 - view 219
- switchgroups at-a-glance window 217
- switch-wide tasks 230
- symbols in text 16
- system requirements 27
- systeminfo file 39

T

- tabs
 - alarm notification 64
 - alias 185
 - config 192
 - fabric assist 190
 - filter 26
 - LSAN information 225
 - physical devices 224
 - quickloop 189

- SAN elements 25
- telnet 228
- virtual devices 224
- zone 187
- zoning 169
- tags
 - prefix 96
 - section 95
- technical support, HP 17
- telnet
 - configuring policy 155
 - icon 216
 - on a secure fabric 165
 - opening a session 55, 165
 - policy 148
 - tab 228
- template files 94
- templates, creating and editing 97
- text symbols 16
- threshold behavior, configuring 63
- tools menu 233 to 235
- topology
 - menu 231
 - moving objects 87
 - options 209
- topology view 218
 - configuring options 86
 - layouts 83
 - links 84
 - viewing fabrics with 85
- transaction key file 103
- troubleshooting 195 to 203

U

- uninstalling fabric manager 40
- upgrade paths, supported 37
- upgrading fabric manager 37
- user settings, storing 26

V

- valid domain names 35
- view information, printing 47
- view menu 184, 213 to 225
- view selector bar 24
- viewing
 - alarms 61
 - discovered fabric topologies 86
 - fabric events 57
- views
 - alerts 217
 - customizing 45
 - device ports 221
 - devices 223

- fabric manager [25](#)
- LSAN [223](#)
- LSAN info [224](#)
- overview [215](#)
- portgrid [223](#)
- ports [220](#)
- switches [219](#)
- topology [218](#)
- virtual devices tab [224](#)

W

- websites, HP storage [15](#), [17](#)
- window descriptions, changing [48](#)
- windows
 - at-a-glance [24](#)
 - edit port groups [208](#)
 - edit switch groups [207](#)
 - edit view options [212](#)
 - fabric at-a-glance [216](#)
 - fabric login [206](#)
 - options [208](#)
 - port at-a-glance [217](#)
 - portgroups at-a-glance [217](#)
 - security admin [228](#)
 - switch at-a-glance [216](#)
 - switchgroups at-a-glance [217](#)
- Windows domain authentication [196](#)
- Windows environments [27](#)
- wizards
 - call home configuration [122](#)
 - change management [71](#), [233](#)
 - clone profile [74](#)
 - create secure fabric [150](#)
 - installation [34](#), [202](#)
 - merge secure fabrics [166](#)
 - share devices [142](#), [234](#)

X

- XML file [76](#), [94](#)

Z

- zone tab [187](#)
- zones
 - clearing the database [175](#)
 - creating [177](#)
 - creating aliases for [175](#)
 - creating configuration [169](#)
 - creating fabric assist [180](#)
 - defined [167](#)
 - deleting [178](#)
 - deleting aliases [176](#)
 - deleting configuration [182](#)
 - deleting fabric assist [181](#)
 - disabling configuration [174](#)
 - displaying configuration [171](#)
 - displaying members of [81](#)
 - enabling configuration [173](#)
 - modifying alias members [176](#)
 - modifying members of [177](#)
 - refreshing the database [174](#)
 - renaming [178](#)
 - renaming aliases [176](#)
 - renaming configuration [182](#)
 - renaming fabric assist [181](#)
 - searching for a member [172](#)
- zoning [167](#) to [193](#)
 - adding a WWN to the database [171](#)
 - database [100](#), [170](#)
 - deleting a WWN from the database [171](#)
 - methods [168](#)
 - replacing a WWN in the database [172](#)
 - schemes [168](#)
 - selecting a method [172](#)
 - tabs [169](#)